HOUSE OF COMMONS
CANADA

BEYOND THE NUMBERS: THE FUTURE OF THE SOCIAL INSURANCE NUMBER SYSTEM IN CANADA

Report of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities

Albina Guarnieri, M.P.
Chair

May 1999

Also available on the Parliamentary Internet Parlementaire: http://www.parl.gc.ca

Available from Public Works and Government Services Canada — Publishing, Ottawa, Canada K1A 0S9

BEYOND THE NUMBERS: THE FUTURE OF THE SOCIAL INSURANCE NUMBER SYSTEM IN CANADA

Report of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities

Albina Guarnieri, M.P.
Chair

May 1999

Publications Service

STANDING COMMITTEE ON HUMAN RESOURCES DEVELOPMENT AND THE STATUS OF PERSONS WITH DISABILITIES

CHAIR

Albina Guarnieri

VICE-CHAIRS

Dale Johnston

Bryon Wilfert

MEMBERS

Diane Ablonczy

Bernard Bigras

Bonnie Brown

Brenda Chamberlain

Hec Clouthier

Denis Coderre

Paul Crête

Libby Davies

Jean Dubé

Christiane Gagnon

John Godfrey

Larry McCormick

John O'Reilly

Hon. Andy Scott

Maurice Vellacott

CLERK OF THE COMMITTEE

Danielle Belisle

FROM THE RESEARCH BRANCH OF THE LIBRARY OF PARLIAMENT

Sandra Harder
William Young

THE STANDING COMMITTEE ON HUMAN RESOURCES DEVELOPMENT AND THE STATUS OF PERSONS WITH DISABILITIES

has the honour to present its

FOURTH REPORT

Pursuant to Standing Order 108(2), the Standing Committee on Human Resources Development and the Status of Persons with Disabilities proceeded to the consideration of the Management of the Social Insurance Number. After hearing evidence, the Committee has agreed to report to the House as follows:

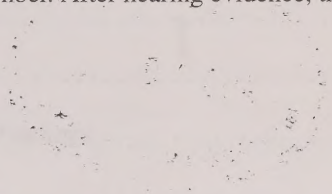
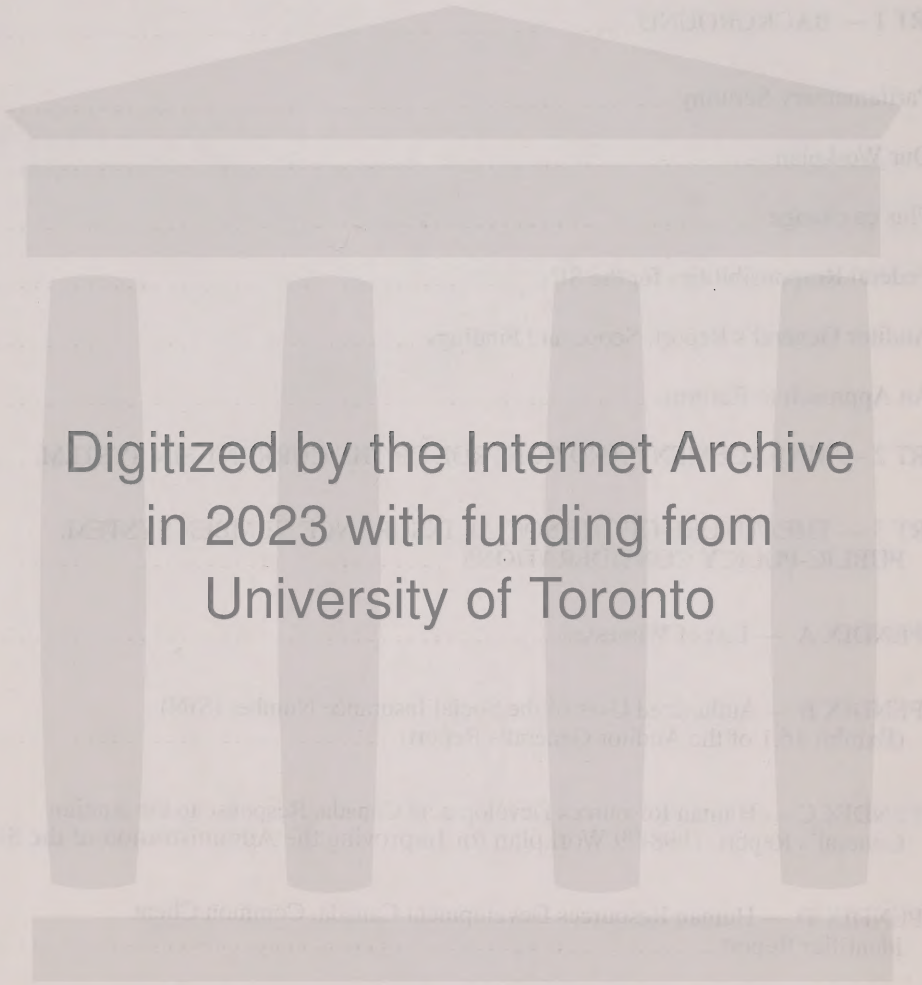


TABLE OF CONTENTS



INTRODUCTION

In the past decades, all Canadians have experienced significant changes in their everyday lives. The unprecedented pace of technological change has had an inescapable impact on communication, business and commerce, education, science, travel and entertainment. Responding to these changes presents great challenges for Canadians, for their elected representatives and for their governments; we are all constantly required to rethink accepted ways of "doing business." As commerce and data management, in both the public and private sectors; moves from paper to cyberspace, Canadians need to feel secure about their personal information and they need reassurance that their privacy is not being sacrificed to efficiency. In many ways, the Social Insurance Number system is a prime example of a government operation that must meet the needs of the 21st century.

Most residents of Canada — even an increasing number of children — carry a small white card in their wallets that bears a nine digit number and no picture. The card — a Social Insurance Number (SIN) card — was issued to them when they first began to work or applied for a government program.

Since then — in some cases over three decades ago — most people have not had occasion to think about their SIN number very often. They enter it on applications, write it in the appropriate space on their income tax forms, and give it to financial institutions when they apply for an account, a loan or a credit card. Perhaps they have been asked for it — and used it — as personal identification when they want to pay by cheque, for example, at their local grocery store or as a guarantee when they rent a movie. The number and the card are both seemingly innocuous; they cannot be used to purchase anything; nor to guarantee admission into any attraction; nor to retrieve money from the bank; nor to qualify for a government program.

Recently, it has become clear that the use of the Social Insurance Number and card, which has not been modernized since its inception in 1964, is causing unintended negative consequences that are felt by thousands — and potentially millions — of residents of Canada. In the past few months, several reports have identified serious problems and sounded the alarm about the evolution and use of the Social Insurance Number and card system. The scope and nature of many of these problems surfaced with the release, in September 1998, of Chapter 16 of the Report of the Auditor General of Canada — *Management of the Social Insurance Number.*[1] Given the wide-ranging implications of his findings, the Auditor General called for parliamentary action to review the administration and broader policy-issues associated with the Social Insurance Card and Number.

In addition to administrative problems with the SIN system, experts have unanimously pointed to the threat posed by the expanded use of the SIN card in the private sector and the extent to which

---

1 Hereafter referred to as the Auditor General's Report or Chapter 16.

the number has strayed beyond its intended purpose as a file number for government programs. This, coupled with rapid technological developments, has raised alarm about the possibility of unauthorized and intrusive data-matching across government departments, within the private sector and possibly even between the public and private sectors. Many of these data matches take place without the card holders' knowledge or informed consent. In combination, these circumstances underscore the importance of placing privacy and the protection of personal information at the centre of all debates about the current operation of the SIN system and its future.

Parliamentary Scrutiny

Last autumn, two parliamentary committees undertook studies that explored various aspects of the administration and policy context of the Social Insurance Number. In late November 1998, the Standing Committee on Human Resources Development and the Status of Persons with Disabilities began a study into the SIN. Subsequently, the House of Commons Standing Committee on Public Accounts reviewed the work of the Auditor General, held hearings on the management of the SIN in Canada and tabled a report in the House of Commons on 4 February 1999. Our own work has led us to reinforce the Auditor General's conclusion: There is a place for a parliamentary perspective on the current SIN system in Canada and an important role for parliamentarians in setting a direction for the future of the SIN system in Canada.

The report of this Committee does not repeat the findings of the Auditor General. We acknowledge the thorough and detailed work done by his office whose team of auditors exposed a number of weaknesses with the way that the SIN and card system in Canada is currently administered. The Auditor General's report also frames a series of important recommendations that set out remedies for the shortcomings of the system, as it presently exists. This Committee concurs with the findings of the AG and we support the content and the spirit of his recommendations.

We recognize, however, that the Auditor General plays a role quite distinct from that of parliamentarians and parliamentary committees. He is charged with examining the operations and efficiency of government programs as they exist; he is not mandated to comment on policy directions for government programs, nor to make policy-related recommendations. Neither does he participate in political debates and decisions; that is for us as elected representatives. The Auditor General himself told us that:

> It is time to review the current roles, objectives and uses of the Social Insurance Number.
>
> The government should determine what it wants to do with the SIN, and should study other possible options at the same time. I also believe it's essential that Parliament play a major role in debating these issues and in finding a satisfactory solution.[2]

In the course of reporting on our deliberations, we want also to acknowledge the work done by our parliamentary colleagues on the Public Accounts Committee. Not surprisingly, their report echoed many of the Auditor General's recommendations and alluded to some of the broader policy-issues that lay before Parliament and indeed before Canadians. The Twentieth Report of the Public Accounts Committee states that:

---

2 Evidence, Meeting No. 43, 4 November 1998, p. 2.

> While the audit [conducted by the Auditor General] uncovered many shortcomings in the administration of the SIN program, these issues are really subordinate to the resolution of the central question concerning the goals and objectives of the Social Insurance Number... Resolution of the SIN mandate is essentially a political issue and will require a decision from the Parliament of Canada.[3]

Apart from our endorsement of this conclusion, we are in considerable agreement with the specific recommendations of the Public Accounts Committee. Our own build upon some of these.

But as the Committee with a mandate to examine and report on issues related to the Department of Human Resources Development, the custodian of the SIN, we have also seen fit to add more "flesh" to the bones of what our colleagues recommended. Moreover, our Committee conducted more extensive hearings and heard from a wider range of interests within and without government. We have used this work as an opportunity to explore, in a preliminary fashion, some of the broader policy-issues.

Nonetheless, while we moved forward, we came to realize that we have not had the time to conduct as in-depth a study of the overarching policy issues of privacy protection and data matching — central to the future of the SIN in Canada — as was undertaken by the former House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities. That Committee spent the better part of a year preparing its report, *Privacy: Where Do We Draw The Line?*, tabled in April 1997. The report, a path-breaking study, identified, explored and analyzed a set of complex issues with remarkable creativity and clarity. That Committee showed a very high level of unanimity in endorsing a comprehensive set of recommendations, based on a call for a Canadian Charter of Privacy Rights.

Unfortunately, the dissolution of Parliament in 1997 eliminated the requirement for the government to prepare a comprehensive response to *Privacy: Where Do We Draw The Line?* which the Human Rights Committee requested. Consequently, the issues and recommendations have remained formally unanswered by the government. Our Committee feels that the depth and breadth of the privacy report frames many of the broad public-policy issues that are part of the debate over the future of the SIN in Canada. Such painstaking and important work should not be overlooked by the government when it prepares a response that addresses our work and our recommendations.

The members of this Committee also acknowledge that Human Resources Development Canada (HRDC) has moved to address many of the issues regarding social insurance numbers raised by the Auditor General. We are confident that the Department has sought to mount a strategy to deal with the immediate administrative concerns around the SIN. However, where we feel it appropriate, we have asked HRDC to adjust its efforts in order to address our concerns. As a way of ensuring accountability, we have also identified time frames and reporting requirements for HRDC. In our

---

3 Twentieth Report of the Standing Committee on Public Accounts, *Chapter 16 of the September 1998 Report of the Auditor General of Canada (The Management of the Social Insurance Number)*, 4 February 1999, p. 7.

view, these adjustments reflect the seriousness of the issues outlined in our report and underscore the extent to which we intend to monitor developments on this file in the immediate future.

This report, therefore, weaves together existing work on measures to reform the SIN system in Canada in the near future and, as well, sets out and frames some of the overarching considerations that should inform the larger debate about future directions.

Our Workplan

We set out on our study with the aim of operating efficiently and neither duplicating nor replicating others' work. The Committee proceeded by holding a series of briefings and round tables that brought together the various governmental and non-governmental bodies with an involvement or interest in the current and future administration of the social insurance numbers, and placing these discussions in the broader policy-context.

Obviously, the Auditor General served as a catalyst for our interest in the issue and he provided us with a detailed briefing about his investigation and conclusions. Then, we invited the various federal bodies with a mandate, or an interest, related to the administration of the Social Insurance Number system and its broader context. This included senior officials from the Department of Human Resources Development, as the "home" of the Social Insurance Number. In addition, the Treasury Board, responsible for the overall guidelines and directives for the use of the Social Insurance Number by federal departments and agencies as well as the Department of Justice, legal counsel and advisor to all federal-government users of the Social Insurance Number, sent representatives. The Privacy Commissioner of Canada, an officer of Parliament like the Auditor General, attended this meeting to provide us with his insights into the use of the Social Insurance Number and the nature of the reforms he thought advisable.

In light of the widespread use of the SIN by other jurisdictions of government and by the private sector, we then held two round tables with as many of the interests as we could gather together. We heard from the privacy commissioners of Ontario and British Columbia, a municipal administrator from the City of Toronto responsible for corporate access and privacy, the Advanced Card Technology Association, the Consumers' Association of Canada, the Canadian Bankers' Association, Action réseau consommateur, Revenue Canada, and Income Security Programs (Human Resources Development Canada). We received several briefs including those from Equifax and written submissions from the Privacy Commissioner of Ontario and the Privacy Commissioner of Canada.

At the end of our study, we invited the Department of Human Resources Development back to engage in a dialogue with us about what we had heard and how it might be applied.

As our work proceeded, we grew increasingly concerned about the threat to personal privacy that exists in the current Social Insurance Number system. We also wanted to explore the implications for personal privacy of proposed changes. We, therefore, concluded by hearing from

security experts who provided us with practical examples about the threats to privacy that currently exist and those that could be eliminated by reforming the system.

Plus ça change

When the SIN system was originally introduced in 1964, much of the debate revolved around the use of the number. Was it just a common file number for several federal government income/entitlement programs or was it a first step on the way to the introduction of a universal identifier for Canadians? The government of the day affirmed that the SIN was not intended to become any form of universal identifier. It was to remain simply a file number to record contributions and entitlements for the Canada/Quebec Pension Plans, Old Age Security and Unemployment Insurance.

Over time, however, the SIN's use has expanded both inside and outside government. First the *Income Tax Act* authorized use of the SIN as an identification number for tax purposes. Later the Act was amended to require the SIN for the purchase and cashing of Canada Savings Bonds. As a result, financial institutions began collecting the SIN of customers for tax reporting. Canadians are now required to have a SIN for their children, if they wish to register them for the newly introduced Registered Education Savings Plan. Today, more than 20 Statutes and Regulations and 7 programs cover authorized use of the SIN[4] (See Appendix B).

The expanded use of the SIN inside government soon paved the way to broader use of the Social Insurance Number in the private sector. Before long, credit bureaus began to use the SIN to run credit checks on potential borrowers. Provincial social programs began using the SIN in the administration of benefits. Employers large and small used it as part of their tracking and accounting system for employee benefits. Mistakenly, the private sector began to look upon the SIN as a piece of identification and property owners asked for it on apartment rental applications, video stores required it as security for movie rentals, universities and colleges requested it on their application forms and pizza places even used it as a customer number for their delivery system. Apart from inappropriate use of the number, its uncontrolled use leaves Canadians vulnerable to serious breaches of their personal privacy that range from data-matching carried out without their knowledge and authorization, to identity theft.

Federal Responsibilities for the SIN

Within the federal government, a number of players have various roles and responsibilities with respect to the SIN. As we have noted, HRDC is the "custodian" of the SIN with responsibility for the issuance of cards, investigating suspected abuse and adjusting regulations if necessary. HRDC also manages the Social Insurance Register (SIR), a record of the personal information that individuals provide when they apply for a card, in a data bank that contains all of the SIN currently in use in Canada. Policy and guidelines that cover the collection and use of the SIN by federal departments

---

4 Auditor General's Report, Chapter 16, p. 16-8.

and agencies, including data-matching, falls within the purview of the Treasury Board. The Department of Justice supports other departments with respect to legal advice for SIN-related questions that arise from the *Privacy Act*, and it also responds to questions from the general public or inquiries regarding the public and private sectors' use of the SIN. The Privacy Commissioner has independent oversight responsibilities arising out of the *Privacy Act* and deals with individuals' complaints about use of the SIN when these relate to infringement of personal privacy. An officer of Parliament like the Auditor General, the Privacy Commissioner reports directly to Parliament.

Auditor General's Report: Scope and Findings

The Auditor General's office undertook an audit of the SIN system in Canada. The audit's objective focused on assessing the "management and control of the SIN to determine if it is efficient and effective and has an appropriate basis in legislation." [5] In order to meet this objective, the audit encompassed the following tasks:

- An examination of the role and use of the SIN in managing social programs and revenue collection;
- An examination of the application process;
- An examination of the management of the Social Insurance Register (SIR);
- An examination of the procedures for the investigation of fraud and abuse;
- Extensive analyses of the SIN databases;
- Discussions with privacy experts and other organizations with interests in the SIN;
- Interviews of officials at HRDC and other federal departments and agencies with responsibilities for the SIN as well as relevant agencies at the provincial level.

The Auditor General's study revealed a number of important problems with the current administration and control of the SIN system in Canada. These problems include:

- The widespread use of the SIN across government departments and programs at the federal and provincial levels of government as well as at the municipal level;
- The extent to which such widespread use contributes to the potential for fraud and abuse of government programs with potentially high financial costs to taxpayers;
- The perception that the SIN is a national identifier and not simply a file number as was its original intent;

---

5 Auditor General's Report, Chapter 16, p. 16-9.

- The extensive use and misuse of the SIN in the private sector (except in Quebec) which increases the potential for fraud, abuse and privacy infringements;
- Significant gaps in the data integrity of the Social Insurance Register;
- Unacceptably low levels of effort dedicated to the investigation of SIN fraud and abuse;
- Minimal penalties for such abuse and fraud;
- A proliferation of temporary SIN cards with no expiry date;
- Problems with the application process including insufficient proof-of-identity procedures;
- The need to re-examine the legal and policy framework for managing the SIN, including the issues of unauthorized data matching and privacy protection.

An Approach to Reform

Our work has led us to conclude that the issues identified by the Auditor General fall into two distinct categories which should be dealt with separately by the government in responding to this and to the other reports. The first of these is the short-term "fixing" of the current system. We are convinced that action on this front should be undertaken as soon as possible. At the same time, we are aware that there are another set of broader public-policy issues that need to be addressed. These concern the question of whether the SIN system needs to be overhauled and/or replaced by a common client identifier. While debate on these latter issues must begin now, we know that a resolution will take longer and require more information and study. We therefore recommend that:

1. **In modifying the Social Insurance Number (SIN) system, the Government of Canada should ensure that it proceeds on two tracks simultaneously:**

   A. **Immediately take steps to correct abuses of the management and control of the current SIN system as reflected in the recommendations in Part 2 of this report; and**

   B. **Address the longer term, broader public-policy issues related to the future of the SIN system, including the issues of privacy and data-matching.**

Our colleagues on the Public Accounts Committee underscored the need to move quickly on the first set of issues and their recommendations echoed much of what the Auditor General's report identified as the immediate imperative to deal with pressing problems and to find workable solutions for the current system. As we also indicated, Human Resources Development Canada, the Department with the lead on management and control of the SIN system, has developed a comprehensive workplan (see Appendix C) to respond to the Auditor General's concerns with the current system. Our recommendations in Part 2 amplify and expand on this work.

With respect to the broader public-policy context, our hearings served to demonstrate both the scope and the complexity of the issues. Part 3 of this report highlights some of these concerns. Rather than make many definitive recommendations in this area, we have framed our report to help identify the kinds of questions that we believe are central to a parliamentary debate on the future of the SIN in Canada.

PART 2 — MANAGEMENT AND CONTROL OF THE CURRENT SIN SYSTEM

The core of current problems with respect to the Social Insurance Number remains a lack of precision and clarity about its purpose. Originally developed as a file number for a few selected government programs, the SIN was never intended to become, or to be thought of as, a national personal identification system for residents of Canada. Yet, that is precisely how the SIN has come to be used. Canada now has a SIN system that is treated akin to a national identifier but contains none of the built-in safeguards that would, or should, govern such a system. Privacy experts all told us that Canada now lives in the worst of all worlds — it possesses a de facto national identifier system with no privacy protection.

A formal legislative mechanism should be put in place to regulate the use of the SIN. Well-proven evidence that this legislative control can work was provided to us by Ontario's Information and Privacy Commissioner who outlined the effectiveness of the 1991 *Ontario Health Cards and Numbers Control Act* in preventing abuse of the Ontario health cards. This Act was implemented and accompanied the release of the new health number in Ontario. Quite simply, the Act states that the health numbers may only be used for certain prescribed medical purposes and it creates an offence accompanied by stiff penalties for use of the card number beyond the bounds of those identified in the Act.[6] In that regard we recommend that:

2. **After appropriate consultations, the Government of Canada should prepare a Social Insurance Number Cards and Numbers Control Act that would set out the legal uses of the existing SIN in both public and private sectors and provide for penalties and fines for the misuse and abuse of the SIN. A draft bill should be tabled with this Committee no later than 31 December 1999.**

Despite claims about the widespread and inappropriate use of the SIN in the private sector, no study substantiates the extent of this inappropriate — or appropriate — use. Before effective solutions can be developed, we concur with the Privacy Commissioner for British Columbia in his conclusion that more attention needs to be directed to the extent of use and abuse of the SIN especially by the private sector. Therefore, we recommend that:

3. **All relevant federal government departments and agencies and the Privacy Commissioner of Canada should work with Statistics Canada to conduct and complete by 31 December 1999, an assessment of the impact and extent of use of the SIN in the public and private sectors. The findings of this study should be**

---

6 Evidence, Meeting No. 47, 3 February 1999, p. 6.

used in the development of a public education campaign regarding the use and abuse of the SIN. (See Recommendation 5)

The Auditor General's report indicates that valid SINs are held by many persons who have no legal status in Canada. In part, this situation arises from the practice of issuing temporary SIN cards (a series of cards that begin with 900) with no expiry date on the card itself or in the file of such numbers in the Social Insurance Register. These cards are issued to seasonal workers, foreign students and non-permanent residents such as refugee claimants. They are also issued to non-Canadian residents who invest in Canada or do their banking in Canada, in order to facilitate the filing of income tax returns. As the report indicates, more than 680,000 temporary cards remain active after a five-year period and the number of temporary SINs issued is more than double the number of non-permanent residents reported by Statistics Canada in 1997.[7] Clearly, this situation requires immediate attention because the proliferation of such cards increases the potential for fraud and abuse. While we do not wish to penalize any holder of an existing temporary SIN card, we recommend that:

4. **HRDC should ensure that by 1 January 2000, all newly issued, temporary SIN cards have a clearly indicated expiry date on them. HRDC should also put in place a mechanism to review all existing temporary cards. While this review is taking place, holders should retain their existing temporary SIN cards. After consultations with the affected groups, but no later than 31 December 1999, a report indicating the results of this review and a plan and timetable for replacing outstanding temporary cards should be tabled with this Committee.**

Our hearings revealed a common conclusion: most Canadians are unaware of the problems linked to the SIN and they are also unaware of the scope and potential for abuse of the SIN. They do not have a clear understanding about the instances where they must provide their SIN, nor are they fully aware about the situations when they can refuse to divulge their number without suffering any consequences. The same situation of operating in ignorance applies to businesses and services in the private sector — both large and small. They often use the SIN as a cheap and convenient bookkeeping tool and business owners and employees may request or require clients and customers to provide their SIN in completely inappropriate situations. Some go so far as to deny a good or service if individuals refuse to divulge their SIN. The Privacy Commissioner for Canada told us that improper use of the SIN by the private sector generates the largest number of complaints received by his office. Individual Canadians, as well as all elements of the private sector, need to understand their rights and responsibilities with respect to the SIN. We therefore recommend that:

5. **Immediately following the passage of the Social Insurance Number Cards and Numbers Control Act, all relevant federal departments and agencies and the Privacy Commissioner of Canada should develop and embark upon a public education campaign regarding SIN in Canada. Such a campaign should:**

---

7 Auditor General's Report, Chapter 16, p. 16-15.

- **Be directed to both the public and businesses, services and organizations that operate in the private sector;**
- **Inform citizens of the legitimate use of their SIN in both the public and the private sectors;**
- **Inform citizens of their legal right to refuse to release their SIN;**
- **Inform businesses, services and organizations of the legal limits of their use of the SIN;**
- **Be made available and accessible to Canadians through a range of media including print, radio and television.**

Steps that will restore the integrity of the Social Insurance Register (SIR) remain central to efforts to straighten out SIN administrative problems. The SIR contains information provided by all applicants for a SIN: basic personal data such as dates and places of birth and death and mother's and father's names. The SIR is managed by National Services, a branch of HRDC that operates out of Bathurst, New Brunswick. The Auditor General found that although the register is generally "well protected and physically secure," the integrity of the data in the register is compromised. For example, between 1965 and 1990 only 1 million deaths were recorded in the SIR compared to 4.4 million deaths in the Canadian population. Moreover, the 1998 database of the SIR recorded 771,000 persons over 90 years of age and 311,000 over 100 years of age, as compared to Statistics Canada's count of 127,000 and 3,000 respectively. For the entire population of Canadians over 20 years of age, the SIR contains more than 26 million entries as compared to Statistics Canada's population estimates of slightly over 22 million for the same age range. This represents a huge difference of about 4 million people. In the face of an inability to reconcile the gap, there is an increased risk of fraud and abuse of the SIN that could represent a significant cost to Canadians in illegal and inappropriate access to federal and provincial programs.[8]

HRDC officials told us that the Department has intensified efforts to address the gap in recorded deaths in the SIR. We also recognize that the provinces and territories have an essential role to play in providing vital statistics information to the SIR. Therefore, we recommend that:

6. **For the strict purpose of maintaining an accurate and up-to-date Social Insurance Register, HRDC should complete consultations with provincial/ territorial governments regarding the controlled and prescribed release of vital statistics (birth, death and name change) between provincial and territorial governments and the federal government by 31 December 1999.**

7. **All exchanges of vital statistics data subsequent to these consultations should be approved by the privacy commissioners of the various jurisdictions involved**

---

8 Auditor General's Report, Chapter 16, p. 16-12.

and the results of the consultations and exchanges reported in HRDC's annual performance report.

An additional concern with respect to the excess of cards in circulation and the procedures for the issuing of new cards arises from the proof-of-identity process for SIN applicants. Until 1976 there was no proof-of-identity procedure at all; anyone who wanted a SIN simply filled in and returned a form. A card with the number was sent by mail. In consequence, as of March 1998, the SIR contained more than 16 million SIN card entries that were unsupported by any secondary identification documents.[9]

We agree with the Auditor General that the managers of the SIR should pay more attention to the proof-of-identity procedures that are currently in place. As his report also found, there are often problems in verifying information contained on documents accepted for SIN applications.

We also take heed of the Privacy Commissioner of Canada's advice that procedures based on efficiency carry potential privacy costs. A recent pilot project of HRDC in New Brunswick provides for online verification of birth, death and name-change information provided by SIN applicants (to avoid fraudulent issuance of a number). But we add a note of caution. We agree that extending this type of identification system to other regions could go some distance in ensuring the accuracy of the SIR and eliminating the issuance of fraudulent new SINs. Nonetheless, we are also aware that the very province where the pilot was conducted does not have a privacy act. After reviewing "Working Group 2: Proof of Identity,"[10] one of HRDC's Working Groups, we recommend that:

8. **HRDC should move immediately to ensure that privacy concerns are given a high priority and submit reports from the Proof-of-Identity Working Group and *all* working groups identified in the Draft Work Plan for Improving the Administration of the SIN, to the Privacy Commissioner for comments.**

9. **HRDC should issue an evaluation report on the New Brunswick Pilot Project and table the report with the Privacy Commissioner of Canada by 30 September 1999. The Privacy Commissioner of Canada should table his comments on the evaluation report with this Committee no less than 30 days thereafter.**

10. **HRDC should restrict any new procedures or programs to guarantee the validity of proof-of-identity documents to information that is clearly required to verify the documents' validity.**

---

9 Auditor General's Report, Chapter 16, p. 16-13 & 16-14.

10 Human Resources Development Canada, *1998-1999 Workplan for Improving the Administration of the SIN*, pp. 4-5.

During our meetings on the SIN system, we heard testimony — sometimes astounding — about the extent and impact of fraud and abuse. Because the SIN is the gateway to a number of federal and provincial programs, the potential cost to taxpayers in over-payments or fraudulent payments is profound. The Auditor General's report identifies several instances where individuals applied for, and received, false SINs in order to file bogus Employment Insurance claims; lease vehicles for fictitiously created companies and then ship the vehicles out of the country for sale overseas; and to apply for, and receive, false GST and income tax refunds. We therefore recommend that:

11. HRDC should put in place a plan that demonstrates its commitment to effective and timely investigations of fraud and abuse of the current SIN system. This plan should be tabled with this Committee by 31 December 1999.

In light of the costs that result from the fraudulent use of the SIN, the federal government, and HRDC in particular, need to pay greater attention to the investigation of possible fraud. We concur with the Auditor General that such investigations are an extremely low priority item within HRDC. This situation should be rectified. One way to address this is to implement a better measure of performance. We believe that the existing performance measurement system at HRDC is inadequate. For example, it emphasizes savings generated from investigations of fraud and abuse to the Employment Insurance account. Any measure must take into account the fact that fraudulent use of the SIN card affects the full range of government programs that use the SIN as a file number (see Appendix B). We therefore recommend that:

12. HRDC should create a new performance measure that demonstrates the accrued savings to the full range of government programs which result from pursuing the fraudulent use of a SIN. The business case for this new measure should be made to Treasury Board during the next round of submissions.

13. HRDC should, based on the outcome of the newly designed measure, assign the appropriate level of human resources to investigate the fraudulent use of a SIN.

14. HRDC should include in its next, and subsequent, Annual Performance Reports to Parliament, a specific section on the management of the Social Insurance Number and the Social Insurance Registry.

Our recommendations thus far reflect those of both the Auditor General and the Public Accounts Committee, particularly with respect to the short-term and immediate problems that deal with the administration of the SIN system. We want responses to our recommendations to reflect the degree of consensus that has been expressed on these issues by all three parliamentary bodies. Actions should be taken swiftly to make the necessary corrections.

15. HRDC should report to Parliament before 30 September 1999 on progress in implementing the 1998-1999 Workplan for Improving the Administration of the SIN (Appendix C of this report).

PART 3 — THE FUTURE OF THE SOCIAL INSURANCE NUMBER SYSTEM: PUBLIC-POLICY CONSIDERATIONS

At the outset of this report, we noted that our hearings on the Social Insurance Number system raised more questions than they answered. Throughout our work, we were constantly confronted by our realization that a solution to the immediate administrative problems identified by the Auditor General's report (dealt with in Part 2) does not tackle the central and fundamental problem within the context of the SIN system. As parliamentarians, we quickly understood that our job is to address the extent to which the SIN system has evolved and strayed from its original intent. Over and over, a variety of witnesses repeated the fundamental importance of clarifying the purpose of the SIN.

The broader public-policy debate, therefore, should attempt to answer the following questions:

1. Should the Social Insurance Number return to its original purpose as an account number to identify files of government programs? If so, can the SIN system be salvaged by following the recommendations set out above or should it be "scrapped" and replaced by a new card — for example, a Millennium card that incorporates new "smart card" technology such as a computer chip or biometric identification?

2. Is it time formally to recognize the SIN's de facto use and to take steps to convert the SIN into a national personal identification number for each and every resident of Canada? Can the introduction of such a card be accompanied by the use of encryption and other "smart card" features that will protect individual privacy?

We were told — and we strongly agree — that any move to turn the SIN into a national identifier must entail widespread political debate as well as adequate and appropriate public input. The creation of a national identification system presents challenges to personal privacy that must be addressed. Personal privacy is too fragile; the guarantees of protection are too weak — and likely to remain so. The temptation for both the public and private sectors to use the data in any national identification system for unintended or unauthorized purposes could be intense and would have to be counterbalanced by adequate technical and legal safeguards.

But we also think that Canadians need an opportunity to weigh the costs and benefits of any significant alteration of, or replacement for, the Social Insurance Number and to debate these in a public forum. Again, the temptation to use a reformed SIN system or a new card for purposes other than those for which it is intended will be very strong. Function-creep based on the demands for "efficiency" is a powerful argument to resist. Individual citizens do not fully understand what they may be giving up. We have already seen examples of this in the recent lawsuit launched, and won, by

the Privacy Commissioner to prevent matching of information collected as Canadians enter or leave the country with unemployment insurance claims. In light of these considerations, we recommend that:

16. HRDC should prepare a report by 31 December 1999 that sets out a series of options — including the associated costs — for improving or replacing the SIN system with an entirely new card system. This report should assess the feasibility of implementing in Canada a SIN administrative model that resembles the Belgium Crossroads Bank model (as discussed in Appendix D of this report).

Our study of the Social Insurance Number has underscored our overall concerns about technology, privacy and data-matching. Witnesses constantly raised these broader issues in our hearings on the SIN. The report of the former House of Commons Standing Committee on Human Rights and the Status of Persons With Disabilities, *Privacy: Where Do We Draw The Line ?*, tabled in April 1997 dealt with these public-policy considerations in detail and at length. That report, the result of an intensive study into issues related to the impact of changing technology on human rights and privacy rights, amplifies and explains many of the concerns that came to animate our members as we looked at the narrower question of the future of the Social Insurance Number system.

In our view, *Privacy: Where Do We Draw The Line?* identifies, discusses, evaluates and recommends measures to deal with these questions and it does so within a framework developed during very extensive public consultations and debate. Due to the timing of the Report's release, there has not been a government response. Consequently:

17. Respecting the existing legislation, we adopt the recommendations and acknowledge the dissenting opinion contained in the report *Privacy: Where Do We Draw The Line?*, the Third report of the House of Commons Standing Committee Human on Rights and the Status of Persons with Disabilities tabled in the House of Commons on 27 April 1997 (Appendix E of this Report). We request a response to these recommendations pursuant to Standing Order 109.

In conclusion, we are left with a series of questions that we have not had as much time to explore as we would have wished.

- If the SIN is "modernized" or "replaced", how will citizens' privacy rights be protected?
- How will we ensure that inappropriate data-matching does not take place?
- What are the best ways to guard Canadians against the rising incidence of identity theft?
- Will we be prepared to respond to the request for a secure and unique identifier for Canadians as more and more commerce takes place electronically?
- As technology expands and becomes more sophisticated, should the office of the federal Privacy Commissioner be given expanded powers to combat intrusions into personal privacy of Canadians and if so, what would the scope of those powers be?

- What are the cost implications of ensuring privacy?
- To what extent are Canadians prepared to shoulder the cost of expensive technology to ensure privacy?
- How do we balance the need for increased efficiency with the rights of individuals to privacy protection?
- How do we deal, in a proactive fashion, with fraud and abuse of the SIN system as well as other forms of card fraud?

These questions represent a sample of the broad public-policy issues that governments will have to deal with in the years ahead. None of these questions has a "yes" or "no" or a "right" or "wrong" answer. They all imply tradeoffs. The basic decisions here, as in the broad public-debate over personal privacy, is the requirement for "informed consent." In order to make these decisions, politicians and Canadians need information and discussion. Too many decisions about the current use of the Social Insurance Number were made by default. This was, and is, not appropriate and should be avoided in the future.

APPENDIX A
List of Witnesses

Associations and Individuals	Date	Meeting
Office of the Auditor General of Canada	November 4, 1998	43
L. Denis Desautels, Auditor General of Canada		
Maurice Laplante, Director		
David Rattray, Assistant Auditor General		
Department of Justice	November 26, 1998	45
Lita Cyr, Counsel		
Brian Jarvis, Legal Counsel		
Human Resources Development Canada		
Jacques Bourdages, Associate Director, National Service		
Hy Braiter, Senior Assistant Deputy Minister		
Bob Nichols, Director		
Office of the Privacy Commissioner of Canada		
Julien Delisle, Executive Director		
Bruce Phillips, Privacy Commissioner of Canada		
Treasury Board of Canada		
Ross Hodgins, Senior Policy Officer		
Ian Sinclair, Director, Information Policy Division		
Advanced Card Technology Association of Canada	February 3, 1999	47
Catherine Johnston, President and CEO		
City of Toronto		
Rita Reynolds, Director, Corporate Access and Privacy Office		
Consumers' Association of Canada		
Jim Savary, Professor		
Information and Privacy Commissioner		
Ann Cavoukian, Information and Privacy Commissioner		
David Flaherty, Information and Privacy Commissioner		
"Action/réseau consommateurs"	February 10, 1999	48
Marie Vallée, Analyst, Policy and regulatory matters, Telecommunications		

Associations and Individuals	Date	Meeting
"Centre de bioéthique, Institut de recherches cliniques de Montréal"	February 10, 1999	48
Pierrot Péladeau, Scientific Coordinator, Telehealth Ethics Program		
Canadian Bankers' Association		
Linda Routledge, Director		
Ted Rowan-Legg, Assistant General Counsel		
Richard Rudderham, Vice-President		
Revenue Canada		
Kathy Turner, Director General		
Royal Canadian Mounted Police		
Victor Gareau, Staff Sergeant		
Human Resources Development Canada	March 3, 1999	49
Jacques Bourdages, Associate Director, National Service		
Dennis Kealey, Director General		
John Knubley, Assistant Deputy Minister, Insurance		
Doug Matheson, Director General, Insurance Service		
Ibis Research Inc.	March 9, 1999	50
Alan Breakspear, President		
Signals 9 Solutions		
Philip Attfield, President		

APPENDIX B
Authorized Uses of the Social Insurance Number (SIN) (Exhibit 16.1 of the Auditor General's Report)

Statutes and Regulations

1. *Budget Implementation Act* (Canada Education Savings Grants)
2. *Canada Elections Act*
3. *Canada Labour Standards Regulations* (*Canada Labour Code*)
4. *Canada Pension Plan Regulations* (*Canada Pension Plan*)
5. *Canada Student Financial Assistance Act*
6. *Canada Student Loans Regulations* (*Canada Student Loans Act*)
7. *Canadian Wheat Board Act*
8. *Employment Insurance Act*
9. *Excise Tax Act* (Part IX)
10. *Garnishment Regulations* (*Family Orders and Agreements Enforcement Assistance Act*)
11. *Farm Income Protection Act*
12. *Gasoline and Aviation Gasoline Excise Tax Application Regulations* (*Excise Tax Act*)
13. *Income Tax Act*
14. *Labour Adjustment Benefits Act*
15. *Old Age Security Regulations* (*Old Age Security Act*)
16. *Tax Rebate Discounting Regulations* (*Tax Rebate Discounting Act*)
17. *Veterans Allowance Regulations* (*War Veterans Allowance Act*)

Programs

1. Income and Health Care Programs (Veterans Affairs Canada)
2. Immigration Adjustment Assistance Program (Citizenship and Immigration Canada)

3. Labour Adjustment Review Board (Human Resources Development Canada)

4. National Dose Registry for Occupational Exposures to Radiation (Health Canada)

5. Rural and Native Housing Program (Canada Mortgage and Housing Corporation)

6. Social Assistance and Economic Development Program (Indian and Northern Affairs Canada)

7. Income Tax Appeals and Adverse Decisions (Revenue Canada)

Source: Department of Justice and Treasury Board Secretariat, June 1998

APPENDIX C

DRAFT

HUMAN RESOURCES DEVELOPMENT CANADA

RESPONSE TO THE AUDITOR GENERAL'S REPORT

1998-99 WORKPLAN FOR IMPROVING THE ADMINISTRATION OF THE SIN

Introduction

The following sets out key elements of a workplan for improving the administration of the SIN, which is in response to the Auditor General's report.

Background

Evolution of the SIN

The Social Insurance Number (SIN) was introduced in 1964, to provide Unemployment Insurance, Canada Pension Plan and Quebec Pension Plan clients with a file number. In 1967, it also became a file identifier for Revenue Canada. The Proof of Identity (PID) Program was established in 1976 to verify the identity and the status in Canada of individuals applying for a SIN. The program's objective was to prevent the assignment to individuals of more than one number and to ensure the integrity of the Social Insurance Registry.

Roles and Responsibilities Regarding the SIN

- **HRD** is the custodian of the SIN: Responsible for issuing SINs, maintaining the SIN data base, investigating abuse, and making regulations.
- The **Treasury Board** is responsible for the policy and guidelines that govern the collection and use of the SIN at the federal level.
- **Privacy Commissioner** investigates complaints about the SIN.
- **Justice** supports other departments in providing legal advice for SIN related questions arising under the *Privacy Act* and responds to general enquiries on the private sector's use of the SIN.

Auditor General's Report

In 1998 the office of the Auditor General (AG) of Canada carried out a thorough review of the Social Insurance Number (SIN). The findings of the audit are contained in Chapter 16 of the AG's report tabled on September 29, 1998.

HRDC has taken the lead on the administrative weaknesses identified in the management of the SIN and, as such, with the assistance of Income Security Programs, Statistics Canada and Revenue Canada, has identified a number of short-term action items:

- February, 1999 — Assistant Deputy Minister to meet with Social Services and Vital Statistics counterparts
- March, 1999 — Add OAS Mortality and certified data from active data base
- April, 1999 — Revenue Canada file of all active SIN's on IDENT database

- May — June 1999 Add OAS Mortality and certified data from archived files
  Determine SIN activity from OAS archived files

Key Administrative Issues Raised by the Auditor General

- Human Resources Development has been administering the SIN in accordance with the intent of its legal framework whereby the SIN is intended to be a file identifier (account number) for certain federal government programs. However, the public often perceives the SIN to be a personal identifier or even an identity card.
- The use of the SIN outside the federal domain has evolved beyond the intent of the Treasury Board policy established in 1989, aimed at preventing it from becoming a national personal identifier. Their audit found that the SIN has become the common numerical identifier both inside and outside the federal government for a wide range of income related transactions and benefits, among other uses.
- However, the SIN program has a number of weaknesses relating to data integrity, proof of identity, SIN penalties, SIN investigations and the SIN card (For more detail, refer to Appendix "A" — actual comments from the Auditor General's Report). As the use of the SIN has become more widespread, these weaknesses have grown in importance.

HRDC Response: Key Challenges

In response to the Auditor General's report, HRDC has identified five key administrative challenges:

1. Address issues related to the integrity of the data on the Social Insurance Register.
2. Examine the Proof of Identity program and its scope.
3. Consider how best to improve the quality and number of SIN investigations.
4. How to better prevent SIN fraud including the possibility of administrative penalties.
5. Explore changes to the SIN card:

   - Expiry date for temporary SINs

   - More secure SIN card if government chooses to introduce a personal identifier.

HRD Workplan

HRD, aware of its responsibilities related to the issuance of Social Insurance Numbers, maintenance of the Social Insurance Register, and investigation of suspected abuse has developed a workplan based on the activities of five working groups:

Working Group 1: Data Integrity

- **What:** Improve integrity of data on Social Insurance Register (SIR). Not all deaths are recorded nor departures from the country.
- **Who:** HRD: National Services (lead), Insurance Services, Systems, Income Security, Investigation and Control; and Revenue Canada
- **How:**
  - Reduce number of uncertified accounts through access to other programs with Proof of Identity.
  - Annotate "unused" SINs e.g. no action at RC, CPP, EI etc.
  - Increase number of recorded deaths through possible access to provincial data, Statistics Canada, External Affairs etc.
- **Possible Outcomes:**
  - MOUs and Agreements to access other federal or provincial birth, death and name change data.
  - Data matching to address backlog of mortality data.
  - Access to EI, Income Security and Revenue data to determine if SIN remains in active use.
- **Milestones:**

November, 1998	Complete formation of project team First draft Terms of Reference document
December, 1998	Determine contents of SIN data base Letter to Statistics Canada requesting mortality data
March, 1999	Add OAS Mortality data from active data base Determine SIN activity from OAS active data base Revenue Canada file of all active SINs on IDENT database
April, 1999	Determine sources of additional birth and mortality data Implementation strategy for acquiring additional birth and mortality data
May, 1999	Address remaining uncertified accounts Add OAS Mortality data from archived files Determine SIN activity from OAS archived files
July, 1999	First draft report

Working Group 2: Proof of Identity

- **What:** Review Proof of Identity process used to support SIN application. No PID required until 1976 as SIN viewed simply as file identification number.
- **Who:** HRD: National Services (lead), Insurance Services, Investigation and Control, Income Security; Citizenship and Immigration and Revenue Canada.

- **How:**
  - Review primary documents used to support SIN application.
  - Review SIN application processing procedures.
  - Review PID procedures used in other programs and jurisdictions.
  - Recommend new PID.
  - Implement tighter controls.
- **Possible Outcomes:**

  1. Additional documentation of identity required at time of application.

  2. Verification of documentation at originating source e.g. Link to Provincial Vital Statistics to verify birth data.

- **Milestones:**

□	November, 1998	Complete formation of project team First draft Terms of Reference document
□	December, 1999	Implement procedures to track fraudulent identities
□	January, 1999	Review PID supporting other programs
□	April, 1999	Consultations and analysis with Provinces and territories
□	March, 1999	Revise SIN handbook and plan for implementation on the Intranet
□	June, 1999	First draft of report

Working Group 3: SIN Penalties

- **What:** To consider how best to prevent SIN fraud including the possibility of administrative penalties for offences because there is currently no effective penalty except when defrauding other programs (EI, Income Security, Revenue Canada etc.).
- **Who:** HRD: Investigation and Control (lead), Benefit Entitlement, Insurance Services, Legal Services and Finance.
- **How:** Determine options for preventing SIN fraud; Review possible legislative changes for SIN fraud including initial recommendations and considering Legal, charter and privacy issues. Regional consultations on impact.
- **Possible Outcome:**

  3. No change.

  4. Increase public awareness.

  5. Implement penalty similar to that in EI.

- **Milestones:**

□	November, 1998	Completion of project team First draft Terms of Reference report
□	December, 1998	Consultations NHQ
□	February, 1999	Regional consultations
□	March, 1999	Consultations on legislative wording
□	April, 1999	Submission to the Commission
□	To be determined	Decision on timetable to enact new legislation

Working Group 4: SIN Investigations

- **What:** Consider how best to prevent SIN fraud; Consider the redesign of Investigation and Control performance indicators to encourage number and quality of SIN investigations.
- **Who:** HRD: Investigation and Control (lead); Consultations with Treasury Board, Revenue Canada and other departments and agencies that may be concerned with SIN fraud.
- **How:** Identify alternatives to the existing system and develop recommendations for Management Committee.
- **Possible Outcome:**

6. Increase public awareness.
7. Treasury Board recognition of value of SIN investigations.
8. More officers assigned to SIN investigations.

- **Milestones:**

□	November, 1998	Completion of project team First draft Terms of Reference report
□	December, 1998	Establish SIN Investigations Monitoring Unit
□	January, 1999	Letter to Regions reinforcing the importance of letters of attestation
□	February, 1999	Consultation and analysis
□	March, 1999	First draft of report Implement Best Practices that would lead to successful prosecutions

Working Group 5: SIN Card

- **What:** To consider expiry date on temporary SIN cards and to investigate upgrading the security features.
- **Who:** HRD: Insurance (lead), National Services, Income Security, Investigation and Control; Revenue Canada and Citizenship and Immigration.

- **How:**
  - Determine scope.
  - Consultations and partnerships.
  - Impact analysis.
  - Implementation strategy
- **Possible Outcome:**
  - No change to SIN card — confirm that it is a file identifier.
  - Add an expiry date to temporary SIN cards only.
  - Issue smart card.
  - Will depend on government decision about future of SIN.
- **Milestones:**

□	November, 1998	Compete formation of project team First draft Terms of Reference report
□	December, 1998	Consultation with Citizenship and Immigration
□	January, 1999	Consultations with authorized SIN users
□	February, 1999	Consultations with partners (e.g. provinces)
□	March, 1999	Consultations with employers, advocacy groups, Privacy and Human rights proponents Consultations with HRD Systems
□	April, 1999	First draft report

Project Co-ordination:

- **What:** To coordinate the activities of all five working groups to ensure coherence and efficiency. To develop overall approach/plan to administrative issues related to the SIN. Examine possible awareness campaign.
- **Who:** Five chairs of working groups; selected participants of other departments (Revenue Canada, Treasury Board Secretariat, Industry Canada, Citizenship and Immigration).
- **How:** Multi-lateral meetings between HRDC, provinces, other government departments; ADM/DM meetings with HRDC and with other departments.
- **Outcome:** Consultation and plan with provinces involving social services departments, vital statistics and privacy coordinated approach and horizontal management of file.
- **Milestones:**

□	Aug. 1998	Presentation to Provincial/Territorial Information Technology directors
□	Sep. 1998	Presentation to F/P/T Directors of Social Services

Dec. 1998	ADM level inter-departmental meeting followed by DM level meeting
Jan. — Mar 1999	Negotiations on MOU with New Brunswick Human Resources on access to the SIR
Spring 1999	Discussions with officials and Deputy Ministers of Social Services, Vital Statistics and Privacy
March, 1999	Review of draft SIN Investigations report
April 1999	Review of draft SIN Penalties report
May, 1999	Table SIN Investigations and SIN Penalties reports with Project Steering Committee
Summer, 1999	Review of draft Data Integrity, PID and SIN Card reports Table Data Integrity, PID and SIN Card reports with Project Steering Committee for decision.

Appendix "A": Actual Comments from the Auditor General's Report

Data Integrity:

1. Significant gap between number of living SIN holders and the size of the Canadian population, a gap of about 3.8 million for those 20 or older:
   - The number of unrecorded deaths is one of the biggest factors in the gap;
   - The number of living Canadians registered in the SIN data base in 1998 remains significantly higher than in Statistics Canada data;
   - Without additional efforts to record deaths, the gaps will continue to grow, along with the potential for confusion and inefficiency and the risk that the identities of deceased individuals could be used for fraudulent activities.
2. Existing sources of information are not fully exploited and more could be done to develop new sources:
   - Data matching with the provinces, territories and in foreign jurisdictions are potential sources of information which could potentially reveal hundreds of thousands of unreported deaths;
   - Even though CPP, Revenue Canada and SIR are sharing more data, the problem of reconciling the various sources remains. For example, Revenue Canada does not provide SIR with corrections it makes to taxpayer files when it notes discrepancies in date of birth, name, etc.
3. Millions of SINs are not certified for identity. There are approximately 11.8 million accounts in the SIR that because of potential for error, misuse and abuse, could cause major concerns to those who make significant use of the SIN.
4. Birth Information is not easily validated with the issuing organization:
   - SIR does not generally confirm the validity of information shown on documents accepted for SIN application with the organizations that issued them;

- Section 6(2) of the *Privacy Act* requires government institutions to ensure that personal information being used for administrative purposes is as accurate, complete and up-to-date as possible.

Proof of Identity:

1. More rigour needed in the Proof of Identity program:
   - Generally, the SIN application process asks for only one identity document and does not have other means to confirm identity such as those of other HRDC programs as well as Passport Canada;
   - In general, mailed applications represent somewhat of a greater risk than in-person applications, because certified photocopies are accepted — which themselves could have been certified fraudulently — and applicants who raise suspicion cannot be questioned;
   - About 20 per cent of total SIN cards issued annually are to replace cards that owners have reported lost, stolen or broken. Controls on this activity need to be improved.
2. Relying mainly on the birth certificate as the foundation of identity has major drawbacks. The birth certificate has the following limitations:
   - Relatively easy to forge or alter;
   - Paper-based so it deteriorates rapidly making information harder to verify;
   - Not linked to the bearer through any special security features;
   - Widespread reliance on documents issued by various agencies creates an inter-dependence. This makes all parties more vulnerable;
   - For the SIN, the extent to which the identity document is validated depends on the ability of HRDC clerks and agents to recognize fraudulent or falsified documents;
   - Design changes in documents, lack of photographs, the mobility of individuals who may be carrying identification produced in many different jurisdictions, all make it increasingly difficult for program staff who review documents to identify forgeries or altered information;
   - The reliability of these documents is not given a rating and so the Department's approach is not tailored according to the quality of identify documents provided by issuing organizations.

SIN Penalties

Penalties resulting from successful SIN investigations are minimal

- The *Employment Insurance Act* states that the penalty for committing any offenses related to the SIN is a fine of up to $1,000 and/or imprisonment for up to one year. Charges under the Criminal Code can also be pressed;
- Very few perpetrators are caught and, even then, the Department rarely brings criminal charges;
- Such low fines do not appear to warrant the considerable time and effort that prosecution entails and their deterrent effect is doubtful. Thus, there is effectively no penalty for activities that

could cause considerable damage to social programs, tax collection, commercial activities and the privacy and security of individual Canadians

SIN Investigations

1. Minimal effort is dedicated to SIN investigations:
    - Since HRDC is responsible for controlling the SIN, it is vital that it conduct proactive and effective investigations in order to prevent, detect and deter abuses that could potentially cost taxpayers many millions of dollars and cause hardship;
    - Identity theft — the illegal use of a person's identity information, including the SIN — is a growing phenomenon in North America;
    - The already small number of SIN investigations continues to decline;
    - The Income Security Programs Branch conducted even fewer Sin-related investigations than the Employment Insurance investigators. Certain Income Security programs may be very vulnerable to fraud.
2. SIN investigations could provide substantial results:
    - There are many types of SIN investigations that lead to investigations. SIN abuses are reported by Revenue Canada, Employment Insurance, Canada Pension Plan, and by provinces. Others are reported by financial institutions.
3. The quality of SIN investigations needs to be improved:
    - In the AG's estimation, fewer than one percent of investigations ultimately generate a strong enough cases to lay charges;
4. Existing performance indicators discourage SIN investigations
    - The savings to other programs that are generated through SIN investigations are not attributed by HRDC to Employment Insurance investigators;
    - The end result of the performance measurement model is that EI investigators give SIN investigations a very low priority;
    - The decline in the number and quality of SIN investigations can also affect the integrity of the SIN data base;

SIN Card

1. Valid SINs are held by thousands of individuals with no legal status in Canada.
    - Since 1976, when the 900-series began, 1,242,000 temporary SINs have been issued. In 1998, some 680,000 temporary SINs remain active and 66 percent of these are over five years old, a long period of time for a number considered temporary;
    - The gap could represent SIN holders who are residing here illegally.
2. The SIN card was not designed to identify the bearer. Thus, the SIN card has no security features that are unique to the bearer (photograph, description etc.) and that could serve to prevent and deter falsification and improper use of the card.

APPENDIX D — HUMAN RESOURCES DEVELOPMENT CANADA, COMMON CLIENT IDENTIFIER REPORT

EXECUTIVE SUMMARY

Background

- In the last two years, under the auspices of HRDC, the federal/provincial/territorial income security programs have undertaken an exploration of the benefits and challenges associated with the possible introduction and use of a common client identifier (CCI) for income security programs in Canada. For the purpose of this study a common client identifier was defined as: *a unique means of identifying an individual in an administrative file.* The purpose of the study was to identify whether there was evidence that a common client identifier could:
    - maintain or enhance privacy and confidentiality;
    - enhance service delivery;
    - streamline program administration; and/or,
    - increase program integrity.
- Options considered for the purposes of this study for use as a common client identifier included:
    - the status quo, i.e. the current Social Insurance Number (SIN);
    - a "modified" SIN; and,
    - a new number.

Current State

- Our research indicated that the provincial and territorial income security jurisdictions are already using the SIN as an administrative identifier for their income security clients. In fact, approximately 90-100% (depending on the jurisdiction) of provincial/territorial income security clients have SIN's.
- Our research also indicated that sharing information between HRDC income security programs and other federal/provincial/territorial programs is common place under the existing legislative

framework. In fact, there are over 100 federal/provincial/territorial agreements in place. The key administrative identifier, in addition to name and date of birth, used to facilitate data matching is the SIN. There is no centralized coordination of all data matching agreements.

- There are current issues arising from the inability to identify and authenticate clients within the income security programs. Access to the SIN Register by the provinces and territories will greatly facilitate verification of the identity of income security and income support applicants.

- Current data matching processes, evolving partly around the Social Insurance Number, fulfill some of the goals of federal/ provincial/territorial income security programs. However, a national system that is specifically designed to achieve the goals of verification of identity and eligibility which are shared by all IS jurisdictions could be more effective.

- Most current data matching is re-active in that it occurs after the fact. An up-front, cross jurisdictional data matching process to validate client identification could minimize inappropriate benefit payment at the outset.

- As reported earlier to the federal/provincial/territorial committee most of the data collected was qualitative rather than quantitative. Very little empirical data was obtained, perhaps due to the sensitivity of the subject matter and/or there simply were no hard numbers available. The cost-benefit analysis was based in large part on the qualitative evidence at hand.

Conclusions

- Based on a review of the attached consolidated report and data gathered to date, there is no compelling case for introducing a common client identifier.

- Our research does indicate, however, that consideration could be given to exploring the possibility of enhancing the current usage of the SIN to further enhance program integrity, improve service delivery and streamline program administration. Steps such as:

    1. under the existing framework, taking full advantage of the SIN register by expanding access to the to the provinces and territories to improve identity authentication.

    2. introducing preventative, up-front data matching, rather than after the fact matching, to validate benefit status, thus minimizing inappropriate benefit payment from occurring at the outset; and,

    3. further investigating the Belgian Crossroads Bank model and its applicability to the Canadian context. The model offers an interesting example to review. It connects eighteen social security agencies, a national register and the European Community register. There is no central repository or warehouse of information. Rather the model allows member agencies to be aware of the existence of files held in other

agencies. All information exchange is reviewed and monitored by an independent committee authorized to review all data exchanges and investigate public complaints.

Next Steps

- There are now several questions/issues that need to be considered:

    1. Based on the work conducted to date, do the federal provincial and territorial income security programs agree with the conclusions?

    2. Do the federal/provincial/territorial programs wish to proceed with further work/study as described in the above conclusions?

    3. If yes, how will this work/study be funded and coordinated?

Common Client Identifier Report

Introduction

Over the last few years there has been growing pressure for governments at all levels and jurisdictions to address the issues surrounding client identifiers. For government, the question of an identifier has become central to the topic of information sharing as a way to provide better services to government clients and/or to reduce government costs.

Service delivery for Human Resources and Development Canada, and for other federal, provincial and municipal departments is currently being redefined. Access to services will continue to be increasingly provided through alternative mechanisms such as kiosks, telephones and the internet. One way to improve service delivery and reduce costs to the public through technology.

The Scope of a Common Client Identifier

Client identifiers can span the spectrum from a national identifier to a program specific file number. An identifier which covers all residents of a country in all programs can be considered a *national client identifier* since it identifies a client in many unrelated government programs. At the other end of the spectrum is a program/context specific number allocated to one program and assigned only to the users of that program. One of the important factors when considering a CCI is to be aware of and actively manage scope.

Scope of the Report

For purposes of this report, a CCI is defined as *a unique means of identifying an individual in an administrative file*. Specifically as a mechanism for uniquely identifying an individual across income security programs, such that each individual is linked to one and only one identity.

Three options were considered:

- the status quo, i.e. the current Social Insurance Number (SIN);
- a "modified" SIN; and,
- a new number.

Objective of the Report

The purpose of this report is to consolidate and synthesize information gathered and determine whether there is evidence that a CCI could:

- maintain or enhance privacy and confidentiality;
- enhance service delivery;

- streamline program administration; and/or,

- increase program integrity.

The purpose of this report is to summarize key findings and next steps and present them in a format conducive to making informed decisions.

Today, the SIN has become the administrative identifier for income security programs in Canada. Approximately 90-100% of income security program participants have and use the SIN as an identifier to interact with the income security programs. The need for a common method for governments to identify and "authenticate" their clients has been discussed by governments at all levels and in many international jurisdictions. Dependable personal identity information is required with almost all interactions with government, from applying for and delivery of financial benefits, linking to other programs and services, maintaining case files, to controlling fraud and error.

Since the late 1980's, data matching and information sharing agreements between jurisdictions have been proliferating, to the point that now there are more than 100 agreements in place between federal/provincial/territorial income security programs, with more pending. These have been enacted under the existing legal framework. The key administrative identifier, in addition to name and birthdate, used to facilitate this data matching is the SIN. Early agreements used name/birthdate matching of information, with the SIN as supporting information. Later agreements tend towards primary use of the SIN for data matching purposes. There is no central overall management, control or coordination of these agreements.

The Social Insurance Number has become the administrative identifier for information sharing between income security programs, Revenue Canada and Immigration programs in Canada. There is no centralized coordination of all data matching agreements.

There are current issues arising from the inability to identify and authenticate clients within the income security programs. In the past provinces and territories have not had the authority to access the information or share the information with the SIN Register (SIR). Although the provinces and territories have legal authority under the Income Tax Act to collect the SIN, access to the SIN Register is controlled by the Employment Insurance legislation.

Recent events have seen SIR policy change in this regard. The Policy branch of the National Services division within HRDC and the Canada Employment Insurance Commission have recently developed a master memorandum of understanding (MOU) that would extend access to the SIN Register to the provinces and territories. Approval of this policy has facilitated the establishment of data sharing agreements between the provinces and territories and the SIN Register. At least one province (New Brunswick) is currently working with the SIN Register staff to draft an information-sharing agreement to allow that province access to SIN Register information.

Access to the SIN Register by the provinces and territories will greatly facilitate verification of the identity of income security and income support applicants.

The current array of data matching and information sharing agreements between federal, provincial, and territorial income security programs in Canada is the administrative response to the need to ensure that benefits are accurate and clients are eligible for those benefits. Each individual data match is targeted to determining one particular bilateral "overlap" of benefit issuance. Each of these "matches" requires a separate legal agreement between the jurisdictions concerned.

Most provinces do not have the full complement of potential matches in place, but all provinces are working in that direction. Each province has started developing agreements with those jurisdictions where the perceived potential for identifying overpayments is highest (i.e., Employment Insurance and neighboring provinces).

Current data matching processes, evolving partly around the Social Insurance Number, fulfill some of the goals of federal/ provincial/territorial income security programs. However, a national system that is specifically designed to achieve the goals of verification of identity and eligibility which are shared by all IS jurisdictions could be more effective.

Most data matching is re-active in that it occurs after the fact. There is no formalized central control and management of data matching across all jurisdictions. There is no one agency accountable for all data matches. Further study could be done in this area and the exploration of a possible solution is proposed later in this report.

Most current data matching is re-active in that it occurs after the fact. An up-front, cross jurisdictional data matching process to validate client identification could minimize inappropriate benefit payment at the outset.

Estimating Costs and Benefits

A number of difficulties arose in attempting to estimate the costs and benefits for a CCI approach. These included:

- The more detailed the implementation plan, the more accurate the cost and benefits estimates become. At a high level, before detailed implementation plans (that address exactly how the CCI will be used) have been defined, only gross estimates are possible.

- Some of the impact of a Common Client Identifier-supported approach to increased data sharing between federal/provincial/territorial programs is in the deterrence factor. Measuring "non-occurrences" of overpayments is notoriously difficult.

- Recouping overpayments that have already occurred (current situation) has a different impact on savings than preventing such overpayments from occurring in the first place. However, estimating the value of immediate reduction in overpayments against the recouping of perhaps the same level of overpayment over time is difficult.

Some applications of a CCI result in clients being determined ineligible on application or identified as ineligible at a later point. This aspect of calculating potential savings is a function of the time that the client *would have received benefits* without the enhanced data sharing process. Many jurisdictions have struggled with the selection of an appropriate time period on which to estimate savings, with some jurisdictions using only a one-month period for the overpayment, and others using various time periods depending on the category of client, and the average time-on-assistance for that category. There is no benchmark for calculating benefits paid out and therefore potential savings estimates vary significantly from jurisdiction to jurisdiction.

- Some of the most significant potential costs and benefits to the implementation of a CCI are intangible: the ease and speed with which service is delivered, the reduction in the "hassle" factor for clients obtaining services and/or increased protection of public funds. Even in the face of a potentially high cost-benefit ratio, the fundamental question remains. Is it worth it from an intangible perspective?

- Due diligence was given to collecting pertinent cost-benefit data to determine whether there was a CCI business case. Surveys and data gathering were conducted with all provinces and territories. Data gathering was also conducted in the international community.

- As reported earlier to the federal/provincial/territorial committee most of the data collected was qualitative rather than quantitative. Very little empirical data was obtained, perhaps due to the sensitivity of the subject matter and/or there simply were no hard numbers available. Cost-benefit analysis was based in large part on the qualitative evidence at hand.

- Many of the estimates made would require verification at a later stage with the appropriate federal/provincial/ territorial officials. In addition, in order to complete the cost-benefit analysis, a number of areas would require additional work regardless. For example:

    1. Workload savings/costs attributable to the implementation of an on-line registration and identification process.

    2. Costs to the Income Security programs (federal/provincial/territorial) to "hook up" to the registry.

    3. Cost of computer hardware for jurisdictions without network capabilities.

Principles for Enhancing Privacy and Confidentiality

This section clarifies the principles and ethical considerations that must underlie the development of any new information sharing system in federal/provincial/territorial income security programs using a CCI.

There are a variety of privacy principles that are in use in the jurisdictions across Canada, including the principles embedded in the federal/provincial/territorial privacy legislation, the principles developed by the CAR working group, OECD fair information practices principles, the Canadian Standards Association. In addition, the Canadian Privacy Commissioner has developed an ethical framework for the development of any new technologies for the delivery of government programs and services (based on the privacy checklist for technology as set out in the Commissioner's 1992-93 annual report).

Although the focus of this project has always been the CCI itself, it is the use of the CCI in conjunction with technology that has the greatest potential impact on privacy. Thus, an ethical framework for technology privacy assessment seems to be the most appropriate framework to assess the CCI options.

1. Beneficence

Technology is a tool to help the government deliver service to individuals, not a tool to transfer control of an individual's data to other persons or agencies or to conduct overt and covert surveillance on its citizens.

2. Non-discrimination

Technology should not limit government services offered to a client or be a condition for clients to have access to government services.

3. Respect

Technology must properly respect the legal and ethical rules pertaining to the rights of the individual to control the usage of their information.

4. Openness/Transparency

Individuals should have the right to refuse to participate in the use of the system; the right to know the nature of the information managed by the system, and the right to understand the nature of the situations likely to develop around the use of the system.

5. Informed Consent

The individual's prior consent is required for all uses of their information and any disclosure of that information to other bodies.

6. Access

Individuals have the right of access to and correction of the information held about them by the system.

7. Matching

Government should ensure that multi-use applications are segregated to prevent merging or cross-matching of data.

8. Gate-Keeping

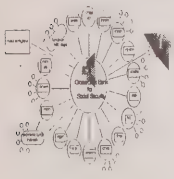
Government has the duty to guarantee the confidentiality of all communications and transmissions surrounding the use of the system.

9. Responsibility

Government has the duty to ensure that those operating and maintaining the system exercise the highest standard of responsibility. Each new application should be monitored for adherence to general privacy principles.

In considering the development of an infrastructure to facilitate information sharing, it would be important to ensure the proper safeguards, both technological, privacy and legal, are in place. In addition, careful attention should be paid to the overall management, control and accountability structures. This framework could be used to assess the privacy impacts.

A Possible Model for the Future



The Belgian Crossroads Bank may be an attractive model to review and to assess in the Canadian context.

The Belgian Crossroads Bank connects eighteen social security agencies as well as the national register and the European Community register. Information exchange takes place either by means of on-line, time-delayed electronic exchange or by tape match.

There is no central repository or data warehouse of information, rather the Crossroads Bank is predicated on a network of social security systems. When an institution requires information it

makes a request to the Crossroads Bank. If the request is legitimate and has received prior approval by the Comité de Surveillance, the Bank verifies whether the information is available. The information is then transferred to the Bank and forwarded to the requesting institution.

This model is based on obligatory participation of all social security institutions. Each individual is identified within the network of income security systems based on a unique identification key (a number). Data storage is decentralized and distributed among the institutions that are responsible for interacting and servicing the client. All information exchanges must go through the Crossroads Bank and be authorized by a "Control Committee". All information exchanges are recorded. The Crossroads Bank contains three reference directories:

1. A person directory identifies where individuals have personal files within the social security institutions and for what periods.

2. A data availability table identifies what type of data is available from each social security institution.

3. An access authorization table indicates what type of data may be transmitted to which institutions for which type of files.

Applying *the Model* to Canada

- For a model to work successfully, in the Canadian context, it would have to:
- respond to the distributed administrative and delivery network of income security programs in Canada;
- provide confirmation of identity in a pro-active manner;
- provide accurate information about an individual's in-pay status on timely basis;
- provide centralized coordination of data matching.
- facilitate accurate data matching and guard against unethical matching;
- address the concerns of the citizenry and the Privacy Commissioners with respect to privacy and confidentiality.

Responding to the Distributed Nature of the Canadian IS System

This model may be suited to meet the needs of the distributed nature in which Canadian programs are delivered among the federal, provincial/territorial and municipal levels of government. The Belgian model does not compromise the delivery structure of the IS programs. In fact, the model pre-supposes that delivery of programs and collection and maintenance of program

information is the responsibility of the particular program within the delivery network. Because information is not centralized in one location but distributed and decentralized, data would continue to be stored and maintained by the various programs and different levels of government that are currently responsible for the information. The different data bases and systems would be linked into the network regardless of their geographic location or level of government. This particular model is predicated on having information reside in the location in which it is managed. Modern technology allows this information to be connected and shared regardless of where it is located or by which level of government it is managed.

Accurate Data Matching and Guarding Against Unethical Matching

All data matching is done via the Crossroads Bank. Most of the "standard" matches are pre-approved and conducted automatically on a scheduled basis resulting in timely and effective data matching. There are several safeguards in place to ensure unethical matches do not occur.

- all matching is done via the Crossroads Bank. There are no matches that occur between individual institutions, thus all matching activity is surveyed;
- all data matches have been pre-approved by the "Comité de Surveillance" (Control Committee);
    - The Control Committee is an independent body appointed by Parliament to review and authorize all data exchanges and review and investigate complaints made by the public. The Committee prepares an annual report of its work to Parliament.
- all matching activity is recorded and tracked; and
- each social security institution has their own security department to monitor and oversee matching activity.

Thus the Belgian model has a built in watch dog function by requiring all matching to occur through the Bank and not on a program to program basis. This watchdog function is already in place in the form of the privacy commissioners in Canada. As a result, any model developed could build on the current role of the federal and provincial/territorial privacy commissioners.

Accurate Information About In-Pay Status

The Crossroads Bank model contains pointer files that indicate where information can be obtained on the in-pay status of clients. This information is assessed prior to benefit payment minimizing the occurrence of mis-payment.

Similarly, in a Canadian model, a pointer file could be created to indicate that an individual is in-pay of a particular benefit. Today, in-pay status information is available under the auspices of the

current data sharing agreements, however each agreement is separate and may not cover the whole spectrum of income security programs.

In a future scenario, if participation of all income security programs is obligatory, then complete information will be available to determine the eligibility of a client to receive benefit payment. This information could be made available up-front reducing incorrect payments before they can occur. If, in a particular case, further information is required, then the institution may go through the central Bank to request additional data on the individual's file if such information sharing is authorized.

Providing Identity Authentication

Access to a central register of basic tombstone data is a cornerstone in the Belgian concept. Information contained in the national register captures life events and basic tombstone information to assist with identity confirmation. However, like all data sharing within this model, the sharing of information has to be pre-approved by the Comité de Surveillance.

In the Canadian context, a similar identity authentication could be validated through the SIN register. With current policy changes that provide access to the SIN register, it is now possible for all jurisdictions to access tombstone information allowing for improved identity verification.

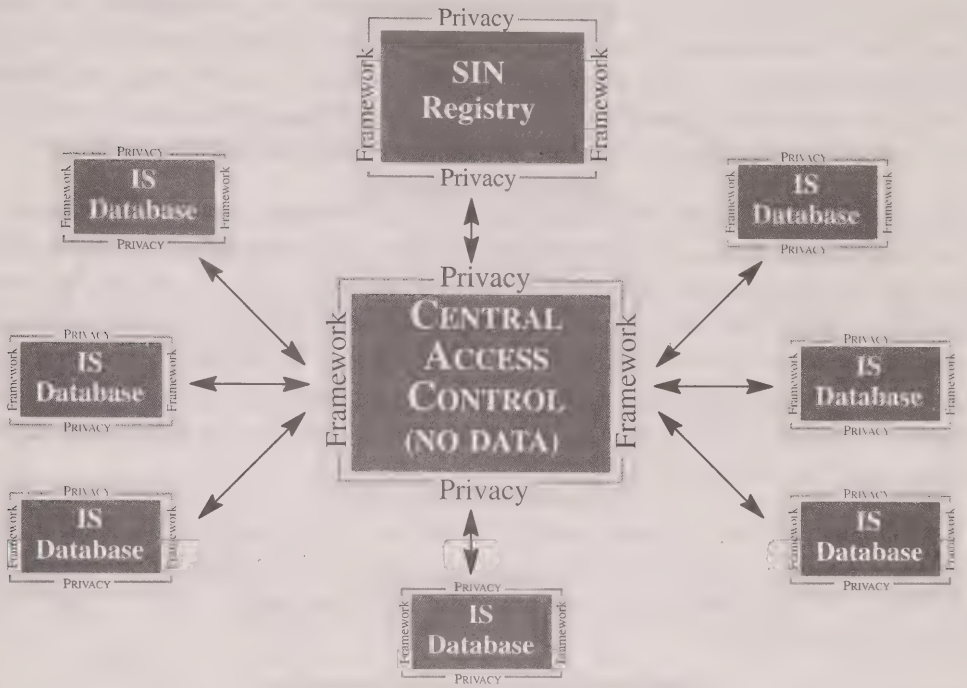
Addresses the Privacy and Confidentiality Concerns

It can be hypothesized that the Belgian model would address many of the concerns and fears of Canadian citizens and Privacy Commissioners with respect to privacy and confidentiality. This model is not predicated upon the creation of a data warehouse, rather a simple network of separate income security systems is joined together under the watchful eye of the Crossroads Bank and the "Control Committee".

As stated earlier, under the current Canadian structure there are a multitude of separate data sharing agreements. There are inter-provincial/territorial data sharing agreements, provincial/territorial-federal agreements and provincial/territorial-municipal arrangements already in place creating a intricate web of non-standardized information sharing agreements. As it stands in most cases today, these agreements have been reviewed and approved by the respective privacy commissioners.

Replacing this web with a formalized model similar to the Belgian model would not radically change the current Canadian structure. Instead of sharing information from institution to institution, this information would pass via a central authority whose role it would be to monitor and ensure regularity and formality to the method in which information is transferred within the income security sphere. This model could improve upon the current framework.

The diagram below provides a pictorial view of a possible future state model for Canada based on the Belgian model.



As stated earlier, this example of a possible future state is "*food-for-thought*". It should not be considered as a solution framework. Further research on the Belgian or similar models is required if this path is to be pursued. A hypothetical description of how this model could function is presented in the following paragraphs.

At the centre of the proposed model sits a Board (perhaps comprised of federal/provincial/territorial privacy commissioners) with several key roles: Their role should include the following functions:

- supervising and directing information security overall;
- reviewing and authorizing/denying each data matching scenario before it occurs;
- handling and responding to complaints; and
- providing information security recommendations.

No client data would be held within the "central access control". It is at the centre where the " pointer files" would be located. Pointer files would indicate in which programs individuals had information (person directory); what type of data was available by each program (information directory); and which program was allowed to access what type of data (authorization directory). Because this information is, in and of itself, a compilation of data, it would be important to ascertain whether it was permissible under today's legislative framework to develop these pointer files or whether legislation or policy changes would be required to create this "new information".

In the hypothetical model, when a new applicant applies for an income security benefit, the applicant would apply to the appropriate program. Program staff would gather basic tombstone and eligibility information from the applicant and verify through the income security program network the individual's identity and in-pay status in other income security programs. Information on the client's in-pay status and personal data would be verified through the central access control (central bank) and the information would be passed back to the host program to determine eligibility based on the results of the data search. Pending approval, the client could then receive benefit payments according to his or her eligibility.

Each program within the income security network would be responsible for maintaining both their client information and program information up-to-date. Each program would continue to be responsible for ensuring that security and privacy of their own specific data is maintained and secured on an on-going basis.

Conclusions

Based on a review of the consolidated report and data gathered to date, there is no compelling case for introducing a common client identifier.

Our research does indicate, however, that consideration could be given to exploring the possibility of enhancing the current usage of the SIN to further enhance program integrity, improve service delivery and streamline program administration. Steps such as:

1. under the existing framework, taking full advantage of the SIN register by expanding access to the to the provinces and territories to improve identity authentication.

2. introducing preventative, up-front data matching, rather than after the fact matching, to validate benefit status, thus minimizing inappropriate benefit payment from occurring at the outset; and,

3. further investigating the Belgian Crossroads Bank model and its applicability to the Canadian context. The model offers an interesting example for to review. It connects eighteen social security agencies, a national register and the European Community register. There is no central repository or warehouse of information. Rather the model allows member agencies to be aware of the existence of files held in other

agencies. All information exchange is reviewed and monitored by an independent committee authorized to review all data exchanges and investigate public complaints.

Next Steps

- There are now several questions/issues that need to be considered:

    1. Based on the work conducted to date, do the federal provincial and territorial income security programs agree with the conclusions?

    2. Do the federal/provincial/territorial programs wish to proceed with further work/study as described in the above conclusions?

    3. If yes, how will this work/study be funded and coordinated?

APPENDIX E — RECOMMENDATIONS from the Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities

Privacy: Where Do We Draw The Line? April 1997

RECOMMENDATION 1

The Committee recommends that the Government of Canada recognize and act upon its responsibility to respect and protect privacy rights in Canada by enacting a declaration of privacy rights to be called the Canadian Charter of Privacy Rights. This Privacy Charter would apply within federal jurisdiction, take precedence over ordinary federal legislation and serve as a benchmark against which the reasonableness of privacy infringing practices and the adequacy of legislation and other regulatory measures would be assessed.

Furthermore, the Committee recommends that the Canadian Charter of Privacy Rights be enacted no later than the 1st of January 2000.

RECOMMENDATION 2

The Committee recommends that the Canadian Charter of Privacy Rights declare and entrench fundamental privacy rights and the responsibilities attaching to these rights. These rights and responsibilities would include, but not necessarily be limited to, the following:

1. Fundamental Privacy Rights and Guarantees

1.1. Everyone is entitled to expect and enjoy:

- **physical, bodily and psychological integrity and privacy;**
- **privacy of personal information;**
- **freedom from surveillance;**
- **privacy of personal communications;**
- **privacy of personal space.**

1.2 Everyone is guaranteed that:

- these privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so;
- violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress.

2. Justification for Exceptions

Exceptions, permitting the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees is reasonable and can be demonstrably justified in a free and democratic society.

3. General Obligations

3.1. The basic duties owed to others to ensure their privacy rights are adequately respected include:

- the duty to secure meaningful consent;
- the duty to take all the steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
- the duty to be accountable;
- the duty to be transparent;
- the duty to use and provide access to privacy-enhancing technologies;
- the duty to build privacy protection features into technological designs.

4. Specific Rights Related to Personal Information

- Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.
- Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.

5. Specific Obligations Related to Informational Privacy

5.1. The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:

- the duty to hold sensitive personal information in trust;
- the duty to limit information collection to what is necessary and justifiable under the circumstances;
- the duty to identify the purpose for which personal information is collected;
- the duty to ensure the information collected is correct and of the highest quality;
- the duty to provide the people whose personal data is collected with access to that information and a means to review and, if they judge it necessary, to correct it;
- the duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;
- the duty to keep personal information only for as long as is necessary and justifiable;
- the duty not to disadvantage people because they elect to exercise their rights to privacy.

RECOMMENDATION 3

The Committee recommends that the Canadian Charter of Privacy Rights declare that to achieve proper respect for privacy rights in Canada the following measures are essential:

- ongoing public discussion and input on matters related to the protection of privacy rights;
- research related to privacy rights and their protection;
- public awareness and education to sensitize everyone to their rights and responsibilities with respect to privacy.

RECOMMENDATION 4

The Committee recommends that the Canadian Charter of Privacy Rights declare that, to ensure the core privacy principles are observed, the following measures must be put in place:

- proper compliance, accountability and enforcement mechanisms;
- appropriate remedies to redress violations of privacy rights.

The Committee further recommends that the Canadian Charter of Privacy Rights declare that the Privacy Commissioner of Canada shall exercise general oversight and protection of privacy rights within areas of federal jurisdiction.

RECOMMENDATION 5

The Committee recommends that the Minister of Justice, in consultation with the Privacy Commissioner of Canada, examine existing federal legislation and regulations, bills and draft regulations for consistency with the Canadian Charter of Privacy Rights and report any inconsistency to Parliament. This report shall be referred to the appropriate parliamentary committee for consideration and recommendations.

The Committee also recommends that the Canadian Charter of Privacy Rights require the Minister of Justice to notify the Privacy Commissioner of Canada of all bills tabled in Parliament and all draft regulations which may have ramifications for privacy.

RECOMMENDATION 6

The Committee recommends that the Government of Canada take a leadership role to ensure that Canadians' privacy rights are accorded equivalent dignity across the country. The Government of Canada should invite the governments of the provinces and territories to work together to develop a complementary and uniform approach to privacy protection across Canada that would accord with the Privacy Charter.

RECOMMENDATION 7

The Committee recommends that the Government of Canada, federal agencies and all Crown corporations identify privacy issues in their respective workplaces and institute appropriate measures that accord with the Privacy Charter to safeguard employees' privacy rights.

RECOMMENDATION 8

The Committee recommends that the Government of Canada introduce into Parliament comprehensive data protection legislation to be known as the Data Protection Act to replace the current *Privacy Act*. This Act must accord with the Privacy Charter and apply to Parliament, all federal government departments, agencies, Crown corporations, boards and commissions, and other institutions, and to all federally regulated businesses and industries. The Data Protection Act shall be enacted no later than the 1st of January 2000.

A broad and open process of public consultation shall precede the introduction of this legislation and provision shall be made in the Act for comprehensive public review of its provisions and operations within five years of the proclamation of the Act, and at regular intervals thereafter.

The Government of Canada shall give due consideration to other data protection models, such as the Canadian Standards Association's Model Code for the Protection of Personal Information and the New Zealand *Privacy Act 1993*, when developing the Data Protection Act. The Data Protection Act shall recognize the role of federally regulated industries in the development of their own privacy codes.

RECOMMENDATION 9

The Committee recommends that the Data Protection Act it proposes contain:

- strict protections against all unnecessary intradepartmental and interdepartmental data matching;
- standards for acceptable data matching practices;
- acceptable data matching practices that comply with the Privacy Charter, in particular the principles of informed consent and transparency.

RECOMMENDATION 10

The Committee recommends that to comply with the proposed Data Protection Act, the Treasury Board Secretariat, a central agency of the federal government must:

- create mandatory data matching guidelines;
- monitor federal government departments for compliance with the new guidelines;
- educate federal departments and employees on what constitutes unnecessary data matching practices.

RECOMMENDATION 11

The Committee recommends that the proposed Data Protection Act shall set out the circumstances under which data sharing between the federal and provincial governments is appropriate.

The Government of Canada should advise the provinces and territories that upon the enactment of the proposed Data Protection Act, all personal information shall only be shared with those provinces that have adequate data protection in place.

RECOMMENDATION 12

The Committee recommends that the proposed Data Protection Act must apply to:

- **any personal information transferred from federal government institutions to the private sector;**
- **any contracts for providing services to federal government institutions.**

RECOMMENDATION 13

The Committee recommends that:

- **the Treasury Board Secretariat take responsibility for monitoring compliance by federal departments and agencies with the proposed Data Protection Act;**
- **the Minister of Industry take responsibility for monitoring compliance by the federally regulated private sector with the proposed Data Protection Act; and**
- **the federal Privacy Commissioner be made responsible for ensuring enforcement of the proposed Data Protection Act and that penalties exist in the proposed act for violations of its provisions.**

RECOMMENDATION 14

The Committee recommends that the Data Protection Act regulate the development, testing (including pilot projects), implementation and application of emerging technologies that have a potential to infringe on the privacy of personal information. These technologies would include, but not be limited to, smart cards and biometric identification systems.

RECOMMENDATION 15

The Committee recommends that the Government of Canada take immediate action to deal with privacy violations and discriminatory treatment that may result from genetic testing including:

- **a review of current policies and practices in the employment, health, insurance and criminal justice sectors;**
- **a review of existing reports and existing and proposed legal instruments (including the draft international covenant on the human genome);**

- consultations with the public;
- the development of legislation that is necessary to deal specifically with the privacy and antidiscrimination issues related to genetic testing.

RECOMMENDATION 16

The Committee recommends that the Government of Canada introduce amendments to the *Criminal Code* that would, to the greatest extent possible, apply the prohibitions against the interception of private communications to surreptitious video surveillance.

RECOMMENDATION 17

The Committee recommends that the Government of Canada, in particular Industry Canada, encourage the development and use of privacy-enhancing technologies by:

- developing partnerships and creating incentives for research and development into privacy-enhancing technologies;
- educating the public and businesses (large and small) about the capacity of privacy-enhancing technologies to protect the personal information of Canadians.

RECOMMENDATION 18

The Committee recommends that the Government of Canada undertake ongoing public awareness and education programs about new technologies and their impact on privacy to ensure that everyone is able to make appropriate decisions regarding their personal privacy and the direction of public policy in the future.

The Committee further recommends that the Government of Canada undertake an ongoing public consultation process that examines and makes recommendations about specific legislative and non-legislative measures that are required to ensure that individuals' privacy is protected as technologies are refined or brought into use.

The Committee further recommends that the Government of Canada initiate ongoing discussions with the provinces with a view to encouraging a common approach to the treatment of these technologies (particularly genetic testing) within different jurisdictions.

RECOMMENDATION 19

- The Committee recommends that the Government of Canada table in Parliament new legislation that would replace the current *Privacy Act*, to be

called An Act Respecting the Office of the Privacy Commissioner of Canada. This act would broaden and strengthen the mandate and powers of the Privacy Commissioner in relation to all issues of privacy within the federal sector. Specifically, it should contain, but not be limited to, provisions that empower the Privacy Commissioner to:

- receive, investigate and settle complaints of alleged privacy invasions;
- initiate his own privacy investigations through the use of privacy audits and technology impact assessments;
- carry out studies relating to privacy and emerging technologies;
- review all government bills, legislation, regulations, delegated legislation, policies and practices that may have an impact on privacy rights and, whenever appropriate, table a privacy impact statement before the House of Commons;
- ensure effective enforcement of the proposed Data Protection Act.

This Act shall apply to Parliament, all federal government departments, agencies, Crown corporations, boards, commissions and government institutions and to the federally regulated private sector.

This Act shall contain complaint review mechanisms such as an administrative tribunal and the provision for judicial review.

RECOMMENDATION 20

The Committee recommends that the introduction of An Act Respecting the Office of the Privacy Commissioner must:

- be preceded by a broad and open public consultation process;
- provide for a comprehensive public review of its provisions and operations within five years of the proclamation of the act and at regular intervals thereafter;
- assign a general public education mandate to the Privacy Commissioner.

RECOMMENDATION 21

The Committee recommends that Parliament provide sufficient resources to the Office of the Privacy Commissioner to adequately carry out its proposed responsibilities.

Dissenting Report to the Report on Privacy Issues produced by the Standing Committee on Human Rights and the Status of Persons with Disabilities

Reform considers it essential for the government to be part of the growing debate over the impact of modern technology on privacy rights and was glad to participate in the recent review performed by the Standing Committee on Human Rights and the Status of Persons with Disabilities.

The opportunity the Committee afforded for Canadians to engage in the public debate was important. Reform, however, is compelled to dissent to the final report issued by the Committee on this study because of the lack of recognition given to the scope of opinion submitted by Canadians from across the country.

Many Canadians recognize the value of some form of regulation or legislation that recognizes the competing interests involved in this complex issue. Many groups, including Industry Canada, recommended a "multi-pronged" approach where responsibility is shared between the government and other interested parties. This would likely include a measure of self-regulation by businesses in the privacy domain.

Instead the government, in standard fashion, has chosen the most narrow and heavy-handed approach by opting to recommend consolidating all power in the federal government, and in particular, under the Privacy Commissioner, greatly expanding the role and responsibilities of the Privacy Commissioner without any apparent consideration of the costs involved or the efficiency of the process.

The Canadian Human Rights Commission (CHRC) seems to mirror many of the functions of the proposed expanded Privacy Commission, but has been ignored as either a source of experience or a possible mechanism for the regulatory process.

According to the government, privacy rights are not congruent with those rights addressed by the CHRC since they do not represent historically-defined discrimination.

However, if the government adjusts this qualification on the definition of the rights addressed by the CHRC, the Commission could then focus on real and present rights' violations. This would facilitate a more equitable approach to rights violations. And if privacy is an "inalienable human right" as it maintains, it could be included in the Commission's portfolio.

Another recommendation of the Committee has potentially serious ramifications on the constitutional distinctions between federal and provincial jurisdictions. In what appears to

be a very heavy-handed approach to enforcing privacy rights, the committee has recommended that federal governments cease data sharing with provinces unless the provinces implement reforms to privacy protection that meet the approval of the federal government. Thus legislation and regulation intended for application in the federal government and federally-regulated organizations will have much farther reaching implications.

The government's interest in enforcing privacy rights also rings hollow in view of its opposition to respecting property rights. With years of pressure and continuing inattention to the area of property rights, why is there now a will to exclusively pursue the related area of privacy?

Several bills illustrate "regulatory creep" and the government's disregard for property and privacy rights:

Bill C-68 significantly weakens Canadians' protection from search and seizure measures, increasing the ease of access of police officers to private property.

Bill C-71 also permits search and seizure without a warrant. While these two bills still maintain a measure of protection regarding dwelling places, Bill C-76, the *Drinking Water Safety Act*, of all pieces of legislation, goes even further. This bill, concerned with the regulation of bottled water, includes provisions for permitting access even to a person's home without a warrant. Little by little, the government is abandoning the historical rights and freedoms of Canadians while trying to claim the high ground by appearing concerned about new, complex issues that are more difficult to define.

Extreme proposals advanced in some circles on behalf of so-called children's rights have also found a friendly ear in some corners of the Liberal government. Such proposals, including the repeal of Section 43 or the privacy rights of children over and above the rights of parents, threaten the protection afforded to children and their families in the private sanctuary of the home. Such infringements threaten to destroy institutions and relationships Canadians have long taken for granted.

The violations of privacy made possible through more and more Liberal legislation sends a contradictory message to the recommendations proposed by the Committee on the limited scope of privacy issues addressed by the Committee. It suggests that the government lacks a comprehensive underlying philosophy that takes into account the priorities of Canadians and reflects the expected level of respect for their rights.

The Reform Party supports the involvement of the government in the public debate over privacy issues. The purpose of public debate, however, is to inform the government of the views and concerns of Canadians.

In consideration of the government report however, the Reform Party recommends greater responsibility and freedom be extended to individuals and businesses to choose and implement standards and measures that also respect the expectations of Canadians.

We recommend a re-examination of the singular proposal to use a greatly expanded Privacy Commission as the structure for the regulatory body.

Finally, we express our reservations over the rush in which the final report was produced which should have allowed more opportunity for careful examination of its proposals and their consequences. The Reform Party trusts that the public consultation proposed by the recommendations will produce results that do indeed represent the wishes and expectations of the broadest possible spectrum of Canadians.

Request for Government Response

Your Committee requests that the Government table a comprehensive response to recommendations 9 and 15 by September 30, 1999 and to the remainder of the report within 150 days in accordance with the provisions of Standing Order 109.

A copy of the relevant Minutes of Proceedings of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities (*Meetings Nos. 45, 47, 48, 49, 50, 51, 53 and 55 which includes this Report*) is tabled.

Respectfully submitted,

Albina Guarnieri, M.P.
Chair

MINUTES OF PROCEEDINGS

TUESDAY, APRIL 27, 1999
(*Meeting No. 55*)

The Standing Committee on Human Resources Development and the Status of Persons with Disabilities met *in camera* at 11:07 a.m. this day, in Room 705, La Promenade Building, the Chair, Albina Guarnieri, presiding.

Members of the Committee present: Diane Ablonczy, Bonnie Brown, Brenda Chamberlain, Hec Clouthier, Paul Crête, John Godfrey, Albina Guarnieri, Dale Johnston, John O'Reilly, The Hon. Andy Scott and Bryon Wilfert.

In attendance: From the Library of Parliament: Sandra Harder and Bill Young, Research Officers.

Pursuant to Standing Order 108(2), consideration of Chapter 16 (Human Resources Development — Management of the Social Insurance Number) of the September 1998 Report of the Auditor General of Canada (*See Minutes of Proceedings of Wednesday, November 4, 1998*)

By unanimous consent,

It was agreed, — That the draft report (as amended) on: *Beyond the Numbers: The Future of the Social Insurance Number System in Canada* be adopted as the Fourth Report of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities.

It was agreed, — That the Clerk be authorized to make such editorial and typographical changes as necessary without changing the substance of the Report.

It was agreed, — That the Chair be authorized to present the Report to the House.

It was agreed, — That, the Committee request that the Government table a comprehensive response to recommendations 9 and 15 by September 30, 1999 and to the remainder of the report within 150 days in accordance with the provisions of Standing Order 109.

It was agreed that a press release be prepared and sent and a press conference be arranged immediately following tabling of the Report in the House.

At 11:28 a.m., the Committee adjourned to the call of the Chair.

Danielle Belisle

Clerk of the Committee

PROCÈS-VERBAL

LE MARDI 27 AVRIL 1999
(*Séance nº 55*)

Le Comité permanent du développement des ressources humaines et de la condition des personnes handicapées se réunit aujourd'hui à huis clos, à 11 h 07, dans la salle 705 de l'édifice La Promenade, sous la présidence de Albina Guarnieri, *présidente*.

Membres du Comité présents : Diane Ablonczy, Bonnie Brown, Brenda Chamberlain, Hec Clouthier, Paul Crête, John Godfrey, Albina Guarnieri, Dale Johnston, John O'Reilly, l'honorable Andy Scott et Bryon Wilfert.

Aussi présents : De la Bibliothèque du Parlement : Sandra Harder et Bill Young, attachés de recherche.

Conformément à l'article 108(2) du Règlement, étude du chapitre 16 (Développement des ressources humaines — La gestion du numéro d'assurance sociale) du rapport du vérificateur général du Canada de septembre 1998 (*voir le procès-verbal du mercredi 4 novembre 1998*).

Du consentement unanime,

Il est convenu, — Que le Comité adopte l'ébauche du rapport (dans sa forme modifiée): *Au-delà des chiffres : l'avenir du numéro d'assurance sociale au Canada*, comme étant le quatrième rapport du Comité permanent du développement des ressources humaines et de la condition des personnes handicapées.

Il est convenu, — Que le greffier soit autorisé à apporter au rapport les changements jugés nécessaires à la rédaction et à la typographie, sans en altérer le fond.

Il est convenu, — Que le président soit autorisé à présenter le rapport à la Chambre.

Il est convenu, — Que le Comité demande au gouvernement de déposer une réponse globale aux recommandations 9 et 15 d'ici le 30 septembre 1999 et à la balance du rapport dans 150 jours, en conformité aux dispositions de l'article 109 du Règlement.

Il est convenu d'envoyer un communiqué et de tenir une conférence de presse immédiatement après le dépôt du rapport à la Chambre.

À 11 h 28, le Comité s'ajourne jusqu'à nouvelle convocation de la présidence.

La greffière du Comité

Danielle Belisle

Demande de réponse du gouvernement

Le Comité demande au gouvernement de déposer une réponse globale aux recommandations 9 et 15 d'ici le 30 septembre 1999 et au reste du rapport dans les 150 jours en conformité des dispositions de l'article 109 du Règlement.

Les Procès-verbaux pertinents du Comité permanent du développement des ressources humaines et de la condition des personnes handicapées (*réunions n^os^ 45, 47, 48, 49, 50, 51, 53 et 55 qui comprend le présent rapport*) sont déposés.

Respectueusement soumis,

La présidente,

Albina Guarnieri, députée

l'éventail très restreint de sujets qu'il a examinés. Elles portent à croire que le gouvernement n'a pas de philosophie fondamentale intégrée qui tienne compte des priorités des Canadiens et traduise le respect dont ils s'attendent à ce que l'on fasse preuve à l'égard de leurs droits.

Le Parti réformiste se réjouit de voir le gouvernement participer au débat public sur les questions relatives à la protection de la vie privée. Il tient cependant à rappeler que le débat public vise à informer le gouvernement des opinions et des craintes des Canadiens.

À la lecture du rapport remis par les membres ministériels du Comité, cependant, le Parti réformiste recommande de laisser aux particuliers et aux entreprises la liberté et la responsabilité d'élaborer et d'appliquer des normes et des mesures qui répondent aux attentes des Canadiens.

Nous recommandons de reconsidérer la proposition fort singulière consistant à élargir considérablement le mandat du Commissariat à la protection de la vie privée afin d'en faire l'autorité réglementante en la matière.

Enfin, nous exprimons des réserves sur l'empressement avec lequel le rapport final a été produit, alors que le Comité aurait dû permettre un examen plus approfondi des propositions du gouvernement et de leurs conséquences. Le Parti réformiste espère que la consultation publique proposée dans les recommandations aboutira à des mesures qui répondront aux voeux et aux attentes du plus grand nombre possible de Canadiens.

personne», comme le gouvernement le soutient, sa protection pourrait aussi relever du Commissariat.

Une autre des recommandations du Comité pourrait avoir des conséquences graves sur la délimitation des champs de compétence constitutionnelle des gouvernements fédéral et provinciaux. Faisant preuve d'un autoritarisme sans précédent en matière de protection du droit à la vie privée, le Comité a recommandé qu'à l'avenir, le fédéral ne partage plus ses données qu'avec les gouvernements provinciaux qui apporteront à leurs lois en matière de protection de la vie privée des modifications approuvées par le gouvernement fédéral, ce qui élargira considérablement le champ d'application de lois et de règlements conçus pour s'appliquer au gouvernement fédéral et aux organismes sous réglementation fédérale.

On ne peut que douter de la volonté du gouvernement fédéral de protéger vraiment le droit à la vie privée quant on sait qu'il refuse de respecter les droits de propriété. Après avoir pendant des années résisté aux pressions et refusé d'examiner la question des droits de propriété, pourquoi se dit-il tout à coup disposé à se charger exclusivement d'un droit connexe, le droit à la vie privée?

Plusieurs projets de loi trahissent un «fluage de la réglementation» et le mépris du gouvernement pour les droits de propriété et le droit à la vie privée.

En effet, le projet de loi C-68 affaiblit considérablement la protection des Canadiens contre la perquisition et les saisies, ce qui facilite aux agents de police l'accès à la propriété privée.

Le projet de loi C-71 autorise lui aussi la perquisition et les saisies sans mandat. Si ces deux mesures protègent encore les logements jusqu'à un certain point, le projet de loi C-76, *Loi sur la sûreté des produits liés à l'eau potable* va encore plus loin, aussi incroyable que cela puisse paraître. Cette mesure, qui réglemente l'embouteillage de l'eau potable, comporte des dispositions qui permettent même d'entrer sans mandat dans le logis d'un citoyen. Petit à petit, le gouvernement abandonne les droits et libertés historiques des Canadiens tout en essayant de s'arroger le droit de tout décider sous prétexte que des problèmes nouveaux et complexes, plus difficiles à cerner, le préoccupent.

Certains membres du gouvernement actuel accueillent par ailleurs avec sympathie les idées extrémistes avancées dans certains cénacles, prétendument au nom des droits des enfants. Ces idées, notamment l'abrogation de l'article 43 ou la primauté des droits des enfants sur ceux des parents, menacent la protection accordée aux enfants et aux familles jusque dans le sanctuaire privé qu'est le foyer familial. De telles atteintes aux droits pourraient détruire des institutions et une hiérarchie des relations humaines que les Canadiens tiennent pour acquises depuis longtemps.

Les atteintes à la vie privée que de plus en plus de mesures libérales rendent possibles envoient un message qui contredit les recommandations faites par le Comité à l'égard de

Rapport dissident adjoint au rapport sur les questions relatives à la vie privée présenté par le Comité permanent des droits de la personne et de la condition des personnes handicapées

Le Parti réformiste considère essentiel que le gouvernement fédéral participe au débat de plus en plus nourri que suscite l'impact de la technologie moderne sur le droit à la vie privée, et il a été heureux de contribuer à l'examen que le Comité permanent des droits de la personne et de la condition des personnes handicapées a récemment fait de la question.

Le Comité a ainsi fourni aux Canadiens une occasion importante de participer au débat public. Toutefois, le Parti réformiste ne peut que se dissocier du rapport final que le Comité a produit à l'issue de cette étude parce qu'il ne fait pas une place suffisante à la diversité des opinions que les Canadiens de l'ensemble du pays ont sur la question.

Beaucoup de Canadiens jugent important de se doter d'une réglementation ou d'une loi qui tienne compte des intérêts concurrents que cette question complexe touche. De nombreux groupes, dont Industrie Canada, ont recommandé une approche «concertée» dans le domaines où le gouvernement et d'autres parties intéressées se partagent la compétence. Une telle approche ferait probablement appel à une certaine mesure d'auto-réglementation de la part des entreprises qui utilisent des renseignements personnels.

Au lieu de cela, le gouvernement a retenu, comme à son habitude, l'approche la plus simpliste et la plus sévère et a choisi de recommander de conférer tous les pouvoirs au gouvernement fédéral et, plus particulièrement, au Commissariat à la protection de la vie privée, dont il accroît ainsi considérablement le rôle et le champ de compétence au mépris apparent de ce que cela coûtera ou de l'efficience du processus que cela implique.

La Commission canadienne des droits de la personne (CCDP) remplit déjà, semble-t-il, beaucoup des fonctions que l'on propose de confier dorénavant au Commissariat, mais le gouvernement a choisi de ne tenir compte ni de l'expérience dont elle pourrait le faire bénéficier, ni du rôle qu'elle pourrait jouer dans l'élaboration d'une réglementation.

Selon le gouvernement, le droit à la vie privée est sans rapport avec les droits que protège la CCDP parce qu'il n'est pas un lieu de discrimination au sens conventionnel de ce terme.

Par contre, si le gouvernement éliminait cette restriction de la définition des droits protégés par la CCDP, cette dernière pourrait alors s'attaquer à des violations bien réelles et actuelles des droits des citoyens. Cela permettrait de donner une suite plus équitable aux violations du droit à la vie privée. Et si le droit à la vie privée est un «droit inaliénable de la

La Loi devra s'appliquer au Parlement, à tous les ministères, organismes, sociétés d'État, conseils et commissions du gouvernement fédéral, ainsi qu'au secteur privé sous réglementation fédérale.

La Loi devra contenir des mécanismes de recours (tribunal administratif et examen judiciaire).

RECOMMANDATION 20

Le Comité recommande que l'adoption de la Loi relative au Commissariat à la protection de la vie privée s'effectue dans le respect des éléments suivants :

- **elle doit être précédée d'une vaste consultation publique;**
- **elle doit prévoir un examen public exhaustif des dispositions et des applications cinq ans après sa promulgation, ainsi qu'à intervalles réguliers par la suite;**
- **elle doit confier au commissaire à la protection de la vie privée du Canada le mandat de sensibiliser le public.**

RECOMMANDATION 21

Le Comité recommande au Parlement de fournir au Commissariat à la protection de la vie privée les ressources nécessaires pour mener à bien son mandat.

- sensibiliser le public, les grandes entreprises et les PME aux possibilités offertes par les technologies en matière de protection des renseignements personnels.

RECOMMANDATION 18

Le Comité recommande que le gouvernement du Canada applique régulièrement des programmes visant à bien renseigner le public sur les nouvelles technologies et sur les incidences qu'elles peuvent excercer sur la vie privée, afin que chacun puisse prendre des décisions éclairées quant à sa vie personnelle et quant à l'orientation des politiques futures du gouvernement.

Le Comité recommande en outre que le gouvernement entreprenne des consultations publiques pour étudier les mesures à caractère législatif ou non devant être prises pour garantir le respect des droits à la protection de la vie privée, à mesure que les technologies apparaissent ou sont perfectionnées.

Le Comité recommande en outre que le gouvernement du Canada encourage, par un dialogue soutenu, les provinces à adopter une approche commune pour le traitement de ces technologies (notamment les tests génétiques).

RECOMMANDATION 19

Le Comité recommande au gouvernement du Canada de remplacer l'actuelle *Loi sur la protection des renseignements personnels* par une nouvelle loi intitulée Loi relative au Commissariat à la protection de la vie privée du Canada, qui étendrait et renforcerait le mandat du commissaire en matière de protection de tous les aspects de la vie privée au gouvernement fédéral. Sans y être limitée, la Loi contiendrait des dispositions qui conféreraient au commissaire les responsabilités suivantes :

- recevoir les plaintes relatives aux présumées infractions, faire enquête et prendre des décisions;

- mener ses enquêtes par le recours à des vérifications et à des évaluations de l'incidence des technologies;

- réviser tous les projets de loi, lois, règlements, décrets-lois, politiques et méthodes susceptibles d'avoir une incidence sur les droits à la protection de la vie privée et soumettre à la Chambre des communes un rapport à ce sujet;

- faire appliquer la Loi sur la protection des données.

- le commissaire à la protection de la vie privée du Canada soit responsable de l'application de la Loi sur la protection des données.

RECOMMANDATION 14

Le Comité recommande que la Loi sur la protection des données réglemente l'élaboration, la mise à l'essai préalable (projets pilotes compris), l'établissement et la mise en application des nouvelles technologies susceptibles d'enfreindre la vie privée. Ces nouvelles technologies comprennent l'identification biométrique et les cartes à puce, mais ne s'y limitent pas.

RECOMMANDATION 15

Le Comité recommande que le gouvernement prenne des mesures immédiates pour remédier aux infractions à la vie privée et aux traitements discriminatoires pouvant résulter des tests génétiques, notamment :

- l'étude des politiques et méthodes actuelles des secteurs de l'emploi, de la santé, de l'assurance et de la justice pénale;
- l'étude des rapports et des instruments légaux actuels et proposés (notamment le projet d'entente internationale sur le génome humain);
- des consultations publiques;
- l'élaboration des lois nécessaires pour contrer les conséquences possibles des tests génétiques en matière de discrimination et de protection de la vie privée.

RECOMMANDATION 16

Le Comité recommande que le gouvernement du Canada modifie le *Code criminel* pour que celui-ci, dans toute la mesure du possible, étende à la surveillance vidéo les dispositions concernant l'interception des communications privées.

RECOMMANDATION 17

Le Comité recommande que le gouvernement du Canada, et en particulier Industrie Canada, encourage les technologies qui favorisent le respect de la vie privée, de la façon suivante :

- développer des partenariats et créer des incitatifs en matière de recherche et de développement visant l'élaboration de technologies équipées de mécanismes favorisant le respect de la vie privée;

RECOMMANDATION 10

Le Comité recommande que, pour garantir le respect de la Loi sur la protection des données, le Secrétariat du Conseil du Trésor, l'un des organes centraux du gouvernement :

- établisse des directives exécutoires en matière de comparaison des données;
- soumette les ministères fédéraux à un contrôle, pour s'assurer qu'ils respectent ces nouvelles directives;
- expliquent clairement aux ministères et aux fonctionnaires fédéraux ce qui est inacceptable en matière de comparaison des données.

RECOMMANDATION 11

Le Comité recommande que la Loi sur la protection des données établisse les circonstances dans lesquelles le partage des renseignements entre les gouvernements fédéral et provinciaux est acceptable.

Le gouvernement du Canada doit aviser les provinces que, dès l'adoption de la loi sur la protection des données, il ne leur communiquera de renseignements personnels que si elles se sont munies d'un mécanisme approprié de protection.

RECOMMANDATION 12

Le Comité recommande que la Loi sur la protection des données s'applique

- à tous les renseignements personnels que le secteur privé a obtenus du gouvernement fédéral;
- à tous les contrats de services passés avec le gouvernement fédéral.

RECOMMANDATION 13

Le Comité recommande que:

- le Secrétariat du Conseil du Trésor soit responsable de vérifier si les ministères et les organismes fédéraux respectent la Loi sur la protection des données;
- le ministre de l'Industrie soit responsable de vérifier si le secteur privé assujetti à la réglementation du gouvernement fédéral respecte la Loi sur la protection des données;

préoccupations concernant la protection de la vie privée, et de prendre les mesures qui s'imposent pour garantir les droits de leurs employés à ce chapitre, conformément à la charte canadienne des droits à la protection de la vie privée.

RECOMMANDATION 8

Le Comité recommande au gouvernement du Canada de présenter au Parlement un texte législatif complet, en remplacement de l'actuelle *Loi sur la protection des renseignements personnels*, désigné sous le titre de Loi fédérale sur la protection des données. Celle-ci devra respecter les dispositions de la Charte canadienne des droits à la protection de la vie privée et s'appliquer au Parlement, à tous les ministères, organismes, sociétés d'État, conseils et commissions du gouvernement fédéral, ainsi qu'à toutes les entreprises et industries assujetties à la réglementation du gouvernement. La Loi devra être promulguée d'ici le 1er janvier de l'an 2000.

La présentation du projet de loi devra être précédée d'une vaste consultation publique et la Loi prévoira un examen public exhaustif cinq ans après la promulgation de la Loi, ainsi qu'à intervalles réguliers par la suite.

Le gouvernement du Canada devrait étudier sérieusement certains modèles, comme le Code type sur la protection des renseignements personnels et la *Loi sur la protection de la vie privée* dont s'est dotée la Nouvelle-Zélande en 1993, avant d'établir la Loi sur la protection des données. Celle-ci devra reconnaître aux entreprises sous réglementation fédérale le rôle d'élaborer leur propre code en matière de protection de la vie privée.

RECOMMANDATION 9

Le Comité recommande que la Loi fédérale sur la protection des données contienne les éléments suivants :

- **des mécanismes de sauvegarde et de contrôles rigoureux contre la comparaison indue des données intra et interministérielle;**
- **des normes définissant les activités acceptables de comparaison;**
- **la définition des activités acceptables de comparaison de données fondée sur les principes énoncés dans la charte proposée sur la protection des renseignements personnels, notamment les principes du consentement éclairé et de la transparence.**

RECOMMANDATION 4

Le Comité recommande que la Charte canadienne des droits à la protection de la vie privée déclare que, pour garantir le respect de principes fondamentaux de protection de la vie privée, les mesures suivantes doivent être mises en place :

- **des mécanismes adéquats d'observation, de reddition de comptes et d'exécution;**
- **des recours appropriés pour réparer toute atteinte à la vie privée.**

Le Comité recommande en outre que la Charte canadienne des droits à la protection de la vie privée déclare que le commissaire à la protection de la vie privée du Canada est responsable de la surveillance et de la protection générale de l'ensemble des droits associés au respect de la vie privée, dans les secteurs de juridiction fédérale.

RECOMMANDATION 5

Le Comité recommande que le ministre de la Justice, en consultation avec le commissaire à la protection de la vie privée du Canada, examine les lois et règlements fédéraux actuellement en vigueur, ainsi que les projets de loi et de règlement, pour s'assurer de leur conformité à la Charte canadienne des droits à la protection de la vie privée, et qu'il signale tout manque de conformité au Parlement. Il recommande également que son rapport soit transmis au comité parlementaire compétent, qui sera chargé de l'étudier et de formuler des recommandations.

Le Comité recommande en outre que la Charte canadienne des droits à la protection de la vie privée oblige le ministre de la Justice d'informer le commissaire à la protection de la vie privée du Canada de tous les projets de loi et de règlement déposés au Parlement susceptibles d'influer sur les droits à la protection de la vie privée.

RECOMMANDATION 6

Le Comité recommande au gouvernement du Canada d'ouvrir la voie et de faire en sorte que les droits des Canadiens à la protection de la vie privée soient respectés de la même façon partout dans le pays. Le gouvernement du Canada devrait inviter les provinces et les territoires à adopter une approche complémentaire et uniforme en cette matière, dans le respect des dispositions de la charte canadienne des droits à la protection de la vie privée.

RECOMMANDATION 7

Le Comité recommande au gouvernement du Canada, aux organismes fédéraux et à toutes les sociétés d'État de recenser, dans leurs milieux de travail respectifs, les

5. Obligations particulières à la protection des renseignements personnels

5.1 Pour que soit garanti le respect des droits à la protection des renseignements personnels, chacun a les obligations suivantes, en plus des obligations générales susmentionnées :

- **l'obligation de détenir en fiducie tout renseignement personnel de nature délicate;**
- **l'obligation de ne recueillir que les renseignements nécessaires et dont la collecte est justifiable;**
- **l'obligation de révéler la raison pour laquelle ces renseignements personnels sont recueillis;**
- **l'obligation de s'assurer que l'information recueillie est exacte et de la meilleure qualité possible;**
- **l'obligation de permettre aux particuliers d'accéder aux renseignements personnels qui les concernent et de les corriger, s'ils le jugent à propos;**
- **l'obligation d'utiliser et de divulguer ces renseignements personnels uniquement pour les raisons indiquées à l'intéressé au moment où il a donné son consentement effectif;**
- **l'obligation de ne pas conserver ces renseignements personnels au-delà de la période pendant laquelle il est nécessaire et justifiable de le faire;**
- **l'obligation de ne pas désavantager les personnes qui décident d'exercer leurs droits à la protection de la vie privée.**

RECOMMANDATION 3

Le Comité recommande que la Charte canadienne des droits à la protection de la vie privée déclare que, pour que soit garanti au Canada, le respect intégral des droits à la protection de la vie privée, les mesures suivantes sont essentielles :

- **consultation du public en permanence sur diverses questions liées à la protection de la vie privée des Canadiens;**
- **recherche sur les droits associés au respect de la vie privée et la protection de ces droits;**
- **sensibilisation et éducation du public, afin que chacun soit conscient de ses droits et responsabilités en matière de protection de la vie privée.**

- protection des communications personnelles;
- protection de l'espace personnel.

1.2 Chacun bénéficie des garanties suivantes :

- ces droits à la protection de la vie privée doivent être respectés par ceux qui prendront les mesures qui s'imposent à cette fin;
- toute atteinte aux droits à la protection de la vie privée, à moins d'être justifiable en vertu du principe d'exception qui suit, doit donner lieu à des mesures adéquates de réparation.

2. Justification des exceptions

Toute exception, autorisant la violation des droits et garanties susmentionnés, ne sera permise que si la justification de cette atteinte aux droits est raisonnable et clairement justifiable, dans le cadre d'une société libre et démocratique.

3. Obligations générales

3.1 Pour que soit garanti le respect des droits à la protection de la vie privée, chacun a les obligations fondamentales suivantes :

- l'obligation d'obtenir le consentement effectif de l'intéressé;
- l'obligation de prendre toutes les mesures qui s'imposent pour respecter adéquatement les droits à la protection de la vie privée d'autrui ou, si l'on ne peut éviter de les enfreindre, de limiter au maximum toute intrusion dans la vie privée;
- l'obligation de rendre des comptes;
- l'obligation de transparence;
- l'obligation d'utiliser des technologies qui favorisent la protection de la vie privée et d'assurer l'accès à ces technologies;
- l'obligation de prévoir des mécanismes de protection de la vie privée dans la conception de nouvelles technologies.

4. Droits particuliers à la protection des renseignements personnels

- Chacun est le titulaire légitime des renseignements personnels qui le concernent, où qu'ils soient détenus, et ce droit est inaliénable.
- Chacun a le droit de s'attendre à jouir, et de jouir de l'anonymat, à moins que la justification de la nécessité d'identifier l'individu ne soit raisonnable.

ANNEXE E — RECOMMANDATIONS
provenant du rapport du Comité permanent des droits de la personne et de la condition des personnes handicapées,

La vie privée : où se situe la frontière?
avril 1997

RECOMMANDATION 1

Le Comité recommande que le gouvernement du Canada reconnaisse et assume la responsabilité qui lui incombe de respecter et de protéger les droits des Canadiens à la protection de la vie privée en adoptant une déclaration des droits à la protection de la vie privée, qu'on nommerait Charte canadienne des droits à la protection de la vie privée. Cette charte viserait l'ensemble du secteur relevant de la compétence fédérale, aurait préséance sur les lois fédérales ordinaires et servirait de repère pour évaluer le caractère raisonnable ou non de pratiques constituant une atteinte à la vie privée, de même que le bien-fondé des lois et autres mesures réglementaires.

De plus, le Comité recommande que la Charte canadienne des droits à la protection de la vie privée soit adoptée au plus tard le 1er janvier de l'an 2000.

RECOMMANDATION 2

Le Comité recommande que la Charte canadienne des droits à la protection de la vie privée déclare et fixe les droits fondamentaux des Canadiens à la protection de la vie privée, ainsi que les responsabilités qui s'y rattachent. Ces droits et responsabilités engloberaient les éléments suivants sans pour autant s'y limiter :

1. Droits et garanties fondamentaux en matière de protection de la vie privée

1.1 Chacun dispose des droits fondamentaux suivants :

- **protection et intégrité matérielle, corporelle et psychologique;**
- **protection des renseignements personnels;**
- **absence de surveillance;**

1. En vertu du cadre existant, optimiser l'IAS en élargissant l'accès aux provinces et territoires dans le but d'améliorer l'authentification de l'identité.

2. Introduire des mesures préventives et initiales de concordance des données, plutôt qu'un appariement après coup, dans le but de valider l'état des prestations et de prévenir les paiements erronés.

3. Étudier davantage le modèle de la banque Carrefour belge et son applicabilité au contexte canadien. Le modèle proposé vaut la peine d'être envisagé. Il relie 18 organismes de la sécurité sociale, un répertoire national et le répertoire de la CE. Il ne prévoit pas de dépôt central ou d'entrepôt des données. Le modèle informe plutôt les organismes membres de l'existence de fichiers auprès des autres organismes. Toute activité d'échange d'information est revue et surveillée par un comité indépendant autorisé à examiner tous les échanges de données et à faire enquête dans les cas de plaintes de la part du public.

Prochaines étapes

Il y a maintenant plusieurs questions et enjeux à aborder :

1. Selon les travaux réalisés jusqu'à présent, les responsables des programmes de sécurité sociale fédéraux, provinciaux et territoriaux sont-ils d'accord avec les conclusions de l'étude?

2. Les responsables des programmes fédéraux, provinciaux et territoriaux souhaitent-ils effectuer d'autres travaux et mener d'autres études conformément aux énoncés précédents?

3. Dans l'affirmative, comment ces travaux et études seraient-ils financés et coordonnés?

Au coeur du modèle proposé réside un « Conseil » (sans doute composé de commissaires à la vie privée fédéraux, provinciaux et territoriaux) ayant plusieurs rôles-clés. Ces rôles devraient inclure ce qui suit :

- superviser et diriger l'ensemble des mesures de sécurité de l'information;
- revoir et autoriser ou refuser chaque scénario d'appariement des données au préalable;
- traiter et résoudre les cas de plaintes;
- fournir des recommandations en matière de sécurité de l'information.

Aucune donnée sur les clients ne serait conservée dans le « contrôle d'accès central ». Il s'agit d'un centre où se trouveraient les « fichiers-repères ». Ces fichiers-repères indiqueraient dans quels programmes les personnes ont de l'information (répertoire des personnes); quel type de données est disponible par programme (répertoire des données); et quel programme est autorisé à accéder à quel type de données (répertoire des autorisations). Puisque cette information est en fait une compilation de données, il serait important de confirmer si le cadre législatif actuel permet l'élaboration de ces fichiers-repères ou s'il faudrait apporter des modifications à la législation ou aux politiques pour créer cette « nouvelle information ».

Dans le modèle hypothétique, lorsqu'un nouveau demandeur s'inscrirait à un des PSR, il ferait une demande dans un programme particulier. Le personnel du programme rassemblerait les données de base et renseignements sur l'admissibilité du demandeur et vérifierait sur le réseau des PSR l'identité de l'individu et l'état de paiement dans les autres PSR. L'information sur l'état de paiement du client et les renseignements personnels à son sujet seraient vérifiés au moyen du contrôle d'accès central (banque centrale). L'information serait ensuite retransmise au programme hôte afin de déterminer l'admissibilité selon les résultats de l'interrogation des données. Sous réserve d'une approbation officielle, le client pourrait ensuite recevoir des paiements de prestations à la lumière de son admissibilité.

Chaque programme du réseau de la sécurité du revenu serait chargé de tenir à jour les données sur ses clients et l'information sur ses activités. Chaque programme continuerait de veiller à ce que la sécurité et le caractère privé de ses données particulières soient assurés et garantis de façon continue.

Conclusions

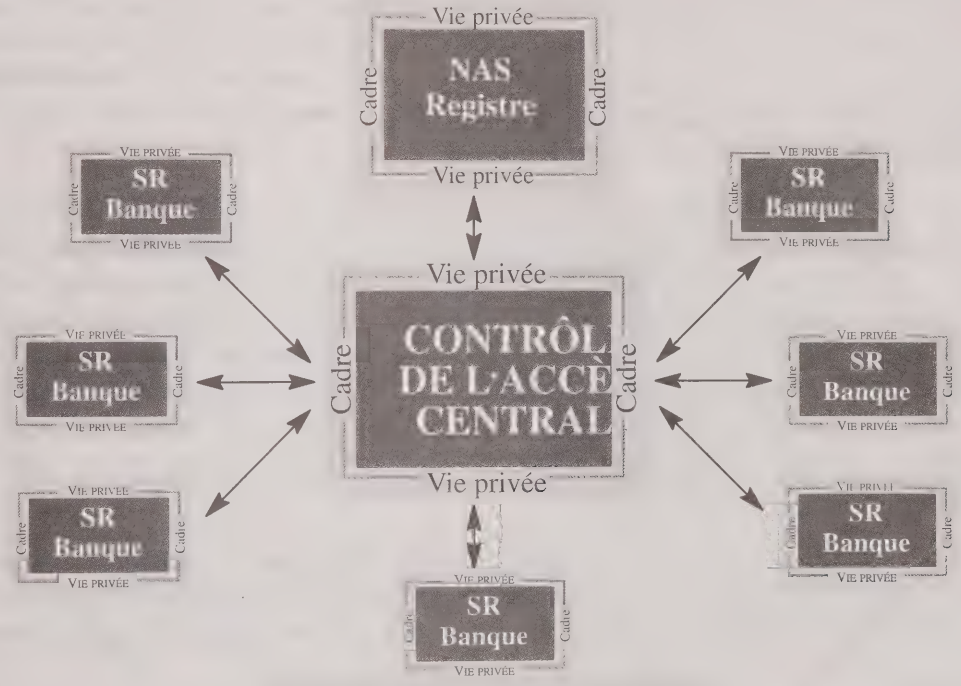
À la lumière de l'examen du rapport consolidé et des données recueillies à ce jour, on ne peut justifier avec fermeté l'introduction d'un CCI.

Les recherches effectuées indiquent néanmoins que DRHC pourrait envisager la possibilité de pousser davantage l'utilisation actuelle du NAS afin d'améliorer l'intégrité des programmes, de rehausser la prestation des services et de simplifier l'administration des programmes. Le Ministère pourrait prendre diverses mesures, notamment :

fédéral, et des accords entre les provinces et territoires et le palier municipal déjà en place, ce qui crée un réseau complexe et non uniforme d'ententes de partage de l'information. Comme c'est le plus souvent le cas de nos jours, ces accords ont été examinés et approuvés par les divers commissaires à la vie privée.

Remplacer ce réseau par un modèle formalisé semblable au modèle belge ne modifierait pas de façon draconienne la structure canadienne en vigueur. Au lieu de partager l'information d'une institution à une autre, cette information transiterait par un pouvoir central dont le rôle serait de surveiller les activités et d'assurer le caractère régulier et formel du mode de transfert de l'information dans le cadre des PSR. Ce modèle pourrait améliorer le cadre actuel.

Le diagramme ci-dessous donne un aperçu visuel d'un modèle canadien éventuel fondé sur le modèle belge.



Tel que mentionné précédemment, cet exemple de modèle éventuel constitue « matière à réflexion ». Il ne devrait pas être envisagé comme une solution absolue. D'autres recherches sur les modèles belge et autres sont requises à cet égard. Une description hypothétique du fonctionnement de ce modèle figure ci-après.

Fournir des données exactes sur l'état des paiements

Le modèle de la banque Carrefour contient des fichiers-repères indiquant où l'on peut obtenir l'information sur l'état des paiements des clients. Cette information est évaluée avant le versement des prestations, ce qui réduit les cas de paiement erroné.

De même, dans un modèle canadien, un fichier-repère pourrait être créé pour indiquer qu'un individu est en situation de paiement d'une prestation particulière. À l'heure actuelle, les données sur l'état des paiements sont accessibles en vertu des accords sur le partage des données en vigueur. Cependant, chacun de ces accords est distinct et peut ne pas englober toute la gamme des PSR.

Dans un scénario éventuel, si la participation de tous les PSR est obligatoire, des données complètes seront donc disponibles afin de déterminer l'admissibilité d'un client à recevoir une prestation. Ces données pourraient être présentées dès le départ, ce qui préviendrait les paiements erronés. Si, dans un cas particulier, d'autres renseignements étaient requis, l'institution pourrait passer par la banque centrale pour demander des renseignements supplémentaires sur le dossier d'une personne si pareil partage d'information est autorisé.

Offrir une possibilité d'authentification de l'identité

L'accès au registre central des données de référence constitue la pierre angulaire du concept belge. L'information contenue dans le registre national saisit les événements de vie et les données de base afin d'aider à confirmer l'identité de chaque personne. Cependant, comme pour tout autre partage de données dans le cadre de ce modèle, le partage de l'information doit être approuvé au préalable par le Comité de surveillance.

Dans le contexte canadien, pareille authentification de l'identité pourrait être validée grâce à l'IAS. Compte tenu des modifications actuelles aux politiques qui donnent accès à l'IAS, il est désormais possible pour toutes les juridictions d'accéder aux données de référence, ce qui améliore les mesures de vérification de l'identité.

Régler les préoccupations en matière de respect de la vie privée et de la confidentialité

On peut présumer que le modèle belge réglerait une bonne partie des préoccupations et craintes des citoyens canadiens et des commissaires à la vie privée en matière de respect de la vie privée et de la confidentialité. Ce modèle n'est nullement fondé sur la création d'un entrepôt de données, mais bien sur un simple réseau de systèmes de sécurité du revenu distincts mais interdépendants sous le regard attentif des responsables de la banque Carrefour et du Comité de surveillance.

Tel qu'il est énoncé antérieurement, la structure canadienne actuelle comprend une multitude d'accords distincts en matière de partage des données. Il y existe des accords de partage de données entre les provinces et territoires, des accords entre les provinces et territoires et le gouvernement

ne sacrifie rien à la structure d'exécution des programmes d'information. En fait, le modèle présuppose que l'exécution des programmes de même que la collecte et la tenue à jour des données sur les programmes sont du ressort de chaque programme au sein du réseau de prestation. Puisque l'information n'est pas centralisée en un seul endroit mais bien répartie et décentralisée, les données continueraient d'être conservées et tenues à jour par les divers programmes et les différents paliers de gouvernement actuellement chargés de cette information. La gamme de bases de données et de systèmes serait reliée au réseau, peu importe l'emplacement géographique ou le palier de gouvernement en cause. Ce modèle particulier est fondé sur l'hypothèse que l'information se trouve au même endroit que le lieu où elle est gérée. La technologie moderne permet toutefois le raccordement et le partage de cette information peu importe l'endroit où elle se trouve ou le palier de gouvernement qui l'administre.

Assurer un appariement exact des données et une protection contre les concordances illicites

Toute concordance de données s'effectue par l'intermédiaire de la banque Carrefour. La plupart des concordances « standard » sont approuvées au préalable et exécutées automatiquement selon un horaire précis, ce qui assure un appariement opportun et efficace des données. Il existe plusieurs protections en vigueur pour éviter les appariements illicites.

- Toutes les concordances s'effectuent au moyen de la banque Carrefour. Aucun appariement ne se fait entre des institutions individuelles, ce qui assure une mainmise sur toute activité d'appariement.

- Toutes les concordances de données sont approuvées au préalable par le Comité de surveillance.

    - Le Comité de surveillance est un organisme indépendant dont les membres sont nommés par le Parlement pour examiner et autoriser tous les échanges de données, en plus d'étudier les plaintes de la part du public et de mener des enquêtes connexes. Le Comité prépare un rapport annuel pour faire état de ses délibérations au Parlement.

- Toute activité d'appariement est enregistrée et fait l'objet d'un suivi.

- Chaque institution de la sécurité sociale possède son propre volet de sécurité chargé de surveiller les activités d'appariement.

Le modèle belge comprend donc une fonction de surveillance intégrée, en ce sens que tout appariement se fait par l'intermédiaire de la banque Carrefour et non au gré des programmes. Au Canada, pareille fonction de surveillance est déjà assurée par les commissaires à la vie privée. Par conséquent, tout modèle à venir pourrait miser sur le rôle actuel de ces commissaires fédéraux, provinciaux et territoriaux.

elle présente une demande à la banque Carrefour. Si la demande est légitime et qu'elle a reçu l'approbation préalable du Comité de surveillance, la Banque vérifie si l'information est disponible. L'information est ensuite transférée à la Banque, puis transmise à l'institution demanderesse.

Ce modèle est basé sur une participation obligatoire de toutes les institutions de la sécurité sociale. Chaque individu est identifié dans le réseau de systèmes de la sécurité du revenu selon un code (ou numéro) unique. L'entreposage des données est décentralisé et réparti parmi les institutions chargées d'interagir et de desservir le client. Tous les échanges de renseignements doivent passer par la banque Carrefour et être autorisés par un « comité de contrôle ». Tous les échanges de renseignements sont enregistrés. La banque Carrefour contient trois répertoires de référence :

1. un répertoire des personnes précise où les individus ont des dossiers personnels auprès des institutions de la sécurité sociale et la période de conservation des documents en question;

2. une table de disponibilité des données précise quel type de données est accessible à partir de chaque institution de la sécurité sociale;

3. une table d'autorisation de l'accès indique le type de données pouvant être transmis à quelles institutions et pour quel type de fichiers.

Application du modèle au Canada

Pour qu'un modèle fonctionne bien dans le contexte canadien, il doit satisfaire aux exigences suivantes :

- être adapté au réseau réparti d'administration et d'exécution des PSR au Canada;
- offrir une confirmation dynamique de l'identité;
- fournir de manière opportune des données exactes sur l'état des prestations individuelles;
- assurer une coordination centralisée des concordances de données;
- faciliter l'appariement exact des données et prémunir contre une concordance non conforme au code de déontologie;
- résoudre les préoccupations des citoyens et des commissaires à la vie privée en matière de respect de la vie privée et de la confidentialité.

Convenir à la nature répartie du réseau des services d'information (SI) canadien

Ce modèle peut servir à combler les besoins du cadre réparti dans lequel s'effectue l'exécution des programmes canadiens aux paliers fédéral, provincial, territorial et municipal. Le modèle belge

6. Accès

Les personnes ont le droit d'accéder à l'information à leur sujet contenue dans le système ainsi que le droit de corriger pareille information.

7. Concordance

Le gouvernement doit s'assurer que les applications à usage multiple sont conservées à part afin de prévenir toute fusion ou comparaison des données.

8. Protection de l'information

Le gouvernement a le devoir de garantir la confidentialité de toutes les communications et transmissions entourant l'utilisation du système.

9. Responsabilité

Le gouvernement a le devoir de s'assurer que les personnes qui exploitent ou entretiennent le système font preuve d'un niveau de responsabilité supérieur. Chaque nouvelle application doit d'ailleurs être surveillée pour ce qui est du respect des grands principes régissant la vie privée.

Au moment d'envisager l'élaboration d'une infrastructure devant faciliter le partage de l'information, il serait important d'assurer l'instauration de mesures de sauvegarde appropriées quant à la technologie, à la vie privée et aux aspects juridiques. De plus, il faut porter une attention particulière aux structures générales de gestion, de contrôle et de reddition de comptes. Ce cadre pourrait être utilisé pour évaluer les répercussions sur la vie privée.

Modèle d'avenir proposé

La banque Carrefour belge peut s'avérer un modèle intéressant à examiner et à évaluer dans le contexte canadien.

Cette banque relie 18 organismes de la sécurité sociale ainsi que le registre national et le registre de la Communauté européenne (CE). L'échange de renseignements se fait en mode direct, par transfert électronique à retardement ou par appariement des bandes.

Il n'existe pas de dépôt central ou d'entrepôt de données. La banque Carrefour est plutôt fondée sur un réseau de systèmes de la sécurité sociale. Lorsqu'une institution a besoin de renseignements,

Une foule de principes relatifs à la vie privée sont en usage dans les diverses juridictions à l'échelle du Canada, y compris les principes intégrés à la législation fédérale/provinciale/territoriale, les principes élaborés par le CRA, les principes derrière les pratiques équitables en matière d'information de l'Organisation de coopération et de développement économiques (OCDE) et les principes de l'Association canadienne de normalisation (CSA). De plus, le Commissariat à la protection de la vie privée du Canada a élaboré un cadre déontologique pour l'élaboration de toute nouvelle technologie d'exécution des programmes et de prestation des services gouvernementaux (à la lumière de la liste de contrôle de la technologie pour ce qui est de la vie privée tel qu'il est stipulé dans le rapport annuel du Commissariat de 1992-1993).

Bien que le point central de ce projet ait toujours été le CCI même, c'est l'utilisation du CCI de pair avec la technologie qui comporte le plus d'incidences éventuelles sur la vie privée. Par conséquent, un cadre déontologique permettant d'évaluer les aspects de la vie privée liés à la technologie semble convenir le mieux à l'évaluation des divers scénarios relatifs au CCI.

1. Bienfaisance

La technologie est un outil permettant au gouvernement d'assurer la prestation des services aux particuliers, et non pas un outil servant à contrôler le transfert des données sur les personnes à d'autres personnes ou organismes ou à mener des activités manifestes ou secrètes de surveillance des citoyens.

2. Non-discrimination

La technologie ne doit pas restreindre les services gouvernementaux offerts à un client ou constituer une condition d'accès des clients à pareils services.

3. Respect

La technologie doit respecter les règles juridiques et déontologiques en matière de droits des personnes afin de contrôler l'utilisation des informations à leur sujet.

4. Ouverture et transparence

Les particuliers devraient avoir le droit de refuser de se prévaloir de tout système, le droit de connaître la nature exacte de l'information administrée par le système en question et le droit de comprendre la nature des situations susceptibles de découler de l'utilisation du système.

5. Consentement éclairé

Le consentement préalable des personnes est requis pour toute utilisation des renseignements à leur sujet et toute divulgation de ces renseignements à des tiers.

Certaines applications du concept de CCI font que les clients sont jugés inadmissibles au moment de la demande initiale ou à une étape ultérieure. Cet aspect du calcul des économies éventuelles est fondé sur la période au cours de laquelle le client a reçu des prestations sans le processus amélioré de partage des données. De nombreuses juridictions se sont butées à la sélection d'une période appropriée sur laquelle baser les estimations d'économies : certaines juridictions utilisent une période d'un mois pour les trop-payés, et d'autres se fondent sur des périodes diverses selon la catégorie de client et la période moyenne de validité de l'aide dans cette catégorie. Il n'existe aucune donnée-repère pour le calcul des prestations versées. Les estimations d'économies éventuelles varient donc grandement d'une juridiction à l'autre.

- Certains des coûts-avantages éventuels les plus importants liés à la mise en oeuvre d'un concept de CCI sont intangibles : la facilité et la rapidité de la prestation de services, la réduction du « fardeau » des clients à obtenir les services et une protection accrue des deniers publics. Malgré la possibilité d'un rapport coûts-avantages élevé, la question fondamentale demeure la suivante : « Le jeu en vaut-il la chandelle d'un point de vue intangible? »

- Une diligence raisonnable a été accordée à la collecte des données pertinentes aux coûts-avantages afin de déterminer s'il existait une analyse de rentabilisation du concept de CCI. Des enquêtes et compilations de données ont été réalisées à l'échelle des provinces et territoires. Des données ont également été rassemblées auprès de la communauté internationale.

- Tel qu'il a été signalé antérieurement au comité fédéral-provincial-territorial, la plupart des données recueillies étaient de nature qualitative plutôt que quantitative. Très peu de données empiriques ont été obtenues, peut-être à cause du caractère délicat du sujet ou de l'absence de chiffres absolus. Une analyse des coûts-avantages a été fondée en grande partie sur les preuves qualitatives disponibles.

- Un grand nombre des estimations exigeraient une vérification ultérieure auprès des représentants fédéraux, provinciaux et territoriaux appropriés. En outre, afin de mener à bien l'analyse des coûts-avantages, un certain nombre de points nécessiteraient des travaux supplémentaires, peu importe le scénario retenu. Par exemple :

    1. les économies et les coûts de la charge de travail attribuable à la mise en oeuvre d'un registre à accès direct et d'un processus d'identification;

    2. les coûts de « raccordement » des PSR (fédéraux, provinciaux et territoriaux) au registre;

    3. le coût du matériel informatique pour les juridictions sans capacité de réseau.

Principes d'amélioration du respect de la vie privée et de la confidentialité

La présente section clarifie les principes et aspects déontologiques devant sous-tendre l'élaboration de tout nouveau système de partage d'information dans les PSR fédéraux, provinciaux et territoriaux au moyen d'un CCI.

« chevauchement » bilatéral particulier en matière d'émission de prestations. Chacune de ces « concordances » exige une entente légale distincte entre les juridictions en cause.

La plupart des provinces ne bénéficient pas d'une gamme complète de possibilités de concordances en place, mais toutes les provinces avancent dans cette direction. Chaque province a commencé à élaborer des ententes avec les juridictions ayant le plus de chances apparentes d'identifier des trop-payés (c.-à-d. l'AE et les programmes provinciaux connexes).

Les processus d'appariement des données actuels, qui évoluent en partie autour du NAS, satisfont à certaines exigences des PSR fédéraux, provinciaux et territoriaux. Cependant, un système national conçu précisément pour atteindre les objectifs de vérification de l'identité et de l'admissibilité qu'ont en commun toutes les juridictions des systèmes d'information (SI) serait plus efficace.

La plupart des concordances de données sont de nature « réactive », c'est-à-dire qu'elles s'effectuent après coup. Il n'existe aucune mesure officielle et centralisée de vérification et de gestion des concordances de données à l'échelle des juridictions. Il n'existe pas non plus d'organisme responsable de la totalité des activités d'appariement des données. D'autres études pourraient être réalisées à cet égard. On propose d'ailleurs une solution de rechange un peu plus loin dans le présent rapport.

La plupart des concordances de données actuelles sont de nature « réactive », c'est-à-dire qu'elles s'effectuent après coup. Un processus de concordance de données initial à l'échelle des juridictions dans le but de valider l'identité des clients permettrait de réduire dès le départ les paiements injustifiés de prestations.

Évaluation des coûts et avantages

Un certain nombre de difficultés sont survenues au cours des activités d'évaluation des coûts et avantages d'une approche fondée sur le principe de code client individuel (CCI), à savoir :

- Plus le plan de mise en oeuvre est détaillé, plus les estimations de coûts et avantages sont précises. À un niveau supérieur, avant que des plans de mise en oeuvre détaillés (abordant avec précision la façon dont le concept de CCI sera utilisé) ne soient définis, seules des approximations brutes sont possibles.

- L'une des incidences du principe de CCI en matière de partage accru des données entre les programmes fédéraux, provinciaux et territoriaux est l'effet de dissuasion. Mesurer les « non-occurrences » de trop-payés s'avère une activité fort difficile.

- Au chapitre des économies à réaliser, recouvrer les trop-payés déjà versés (situation actuelle) constitue un effort différent d'une démarche de prévention initiale de pareils trop-payés. Cependant, il est difficile d'estimer la valeur d'une réduction immédiate des trop-payés par rapport au recouvrement, disons, du même niveau de trop-payés au fil du temps.

nombreuses instances internationales. Des données fiables sur l'identité personnelle sont requises dans presque tous les échanges avec le gouvernement, de la simple demande de prestation à l'acheminement des avantages financiers, en passant par l'établissement de liens avec d'autres programmes et services, la tenue à jour des dossiers de cas et le contrôle des fraudes et erreurs.

Depuis la fin des années 1980, les ententes de concordance des données et de partage de l'information entre les diverses juridictions n'ont cessé de proliférer, à un point tel que l'on dénombre désormais plus de 100 ententes en vigueur entre les PSR fédéraux, provinciaux et territoriaux, sans compter celles en suspens. Ces ententes ont été promulguées dans le cadre juridique existant. Le principal identificateur administratif, outre le nom et la date de naissance, qui sert à faciliter l'appariement des données est le NAS. Les premières ententes se fondaient sur le nom et la date de naissance pour assurer la concordance de l'information, le NAS étant utilisé à titre de donnée d'appoint. Les ententes ultérieures avaient tendance à se servir principalement du NAS à des fins d'appariement de l'information. Il n'existe toutefois aucune gestion, vérification ou coordination centrale et globale de ces ententes.

Le NAS est devenu le principal identificateur administratif pour le partage de l'information entre les PSR, Revenu Canada et les programmes d'immigration au Canada. Il n'existe aucune activité de coordination centralisée de l'ensemble des ententes de concordance des données. Des questions actuelles découlent de l'incapacité à identifier et à authentifier les clients dans le cadre des PSR. Par le passé, les provinces et territoires n'avaient pas à autoriser l'accès à l'information ou le partage des données avec l'Immatriculation aux assurances sociales (IAS). Bien que les provinces et territoires ont en vertu de la Loi de l'impôt sur le revenu le pouvoir juridique de recueillir les données sur les NAS, l'accès à l'IAS est régi par la Loi sur l'assurance-emploi (AE).

Par suite des événements récents, la politique sur l'IAS a évolué à cet égard. Le volet Politique de la Division des services nationaux de DRHC ainsi que la Commission de l'emploi et de l'immigration du Canada (CEIC) ont récemment élaboré un protocole d'entente (PE) type visant l'élargissement de l'accès à l'IAS pour les provinces et territoires. L'adoption de cette politique a facilité l'instauration d'ententes sur le partage des données entre les provinces, les territoires et l'IAS. Au moins une province (Nouveau-Brunswick) travaille actuellement de pair avec le personnel de l'IAS à l'élaboration d'une ébauche d'entente sur le partage de l'information afin de permettre à cette province l'accès aux données de l'IAS.

L'accès à l'IAS par les provinces et territoires facilitera grandement la vérification de l'identité des candidats aux programmes de la sécurité du revenu et aux programmes de soutien du revenu.

La brochette actuelle d'ententes sur la concordance des données et le partage de l'information entre les PSR fédéraux, provinciaux et territoriaux au Canada constitue la réponse administrative au besoin d'assurer l'exactitude des prestations et l'admissibilité des clients à pareils avantages. Chaque démarche d'appariement des données est ciblée de manière à déterminer un

d'un pays et l'ensemble des programmes peut être envisagée comme un code client national puisqu'elle identifie un client dans de nombreux programmes gouvernementaux épars. À l'autre bout du prisme se trouve un numéro propre à un programme ou à un contexte, alloué à un programme particulier et attribué seulement aux utilisateurs de ce programme. L'un des principaux facteurs à retenir : au moment d'envisager un CCI, il faut prendre conscience de la portée et de bien gérer cette dernière.

Portée du rapport

Aux fins du présent rapport, un CCI se définit comme un moyen unique d'identifier une personne individuelle dans le cadre d'un dossier administratif. Plus précisément, il s'agit d'un mécanisme qui permette d'identifier de façon unique une personne à l'échelle des programmes de la sécurité du revenu (PSR), de sorte que cette personne se voit assigner un profil unique.

Trois scénarios ont été envisagés :

- le statu quo, c.-à-d. le numéro d'assurance sociale (NAS) actuel;
- un NAS « modifié »;
- un nouveau numéro.

Objectif du rapport

L'objectif du présent rapport est de consolider et de synthétiser l'information recueillie et de déterminer la mesure dans laquelle un CCI contribuerait à ce qui suit :

- maintenir ou améliorer le respect de la vie privée et de la confidentialité;
- rehausser la prestation des services;
- simplifier l'administration des programmes;
- améliorer l'intégrité des programmes.

Le présent rapport vise essentiellement à résumer les principales constatations et les prochaines étapes tout en les présentant dans un format qui favorise la prise de décisions éclairées.

Situation actuelle

De nos jours, le NAS est devenu la désignation administrative pour les PSR au Canada.De 90 à 100 p. 100 des participants aux PSR possèdent et utilisent un NAS comme code d'accès aux PSR. Le besoin d'une méthode commune permettant aux gouvernements d'identifier et d'« authentifier » leurs clients a fait l'objet de pourparlers de la part de tous les paliers gouvernementaux et de

3. Étudier davantage le modèle de la banque Carrefour belge et son applicabilité au contexte canadien. Le modèle proposé vaut la peine d'être envisagé. Il relie 18 organismes de la sécurité sociale, un répertoire national et le répertoire de la CE. Il ne prévoit pas de dépôt central ou d'entrepôt des données. Le modèle informe plutôt les organismes membres de l'existence de fichiers auprès des autres organismes. Toute activité d'échange d'information est revue et surveillée par un comité indépendant autorisé à examiner tous les échanges de données et à faire enquête dans les cas de plaintes de la part du public.

Prochaines étapes

- Il y a maintenant plusieurs questions et enjeux à aborder :

1. Selon les travaux réalisés jusqu'à présent, les responsables des programmes de sécurité sociale fédéraux, provinciaux et territoriaux sont-ils d'accord avec les conclusions de l'étude?

2. Les responsables des programmes fédéraux, provinciaux et territoriaux souhaitent-ils effectuer d'autres travaux et études conformément aux énoncés précédents?

3. Dans l'affirmative, comment ces travaux et études seront-ils financés et coordonnés

Code client individuel (CCI)

Introduction

Au cours des dernières années, des pressions constantes ont été exercées sur l'ensemble des paliers et juridictions pour régler les questions relatives aux codes clients. Chez les représentants gouvernementaux, la question d'un identificateur occupe maintenant une place prépondérante au chapitre du partage de l'information, à titre d'outil permettant de fournir des services améliorés aux clients gouvernementaux et de réduire les coûts pour les instances gouvernementales.

Développement des ressources humaines Canada (DRHC) et d'autres ministères fédéraux, provinciaux et municipaux sont à revoir leur définition de la prestation des services. L'accès à pareils services continuera d'être offert de plus en plus au moyen de solutions de rechange telles que les kiosques, la téléphonie et le réseau Internet. La technologie, c'est une façon d'améliorer la prestation des services et de réduire les coûts pour le public.

Portée d'un CCI

Les codes clients peuvent prendre diverses formes : depuis un identificateur national jusqu'à un numéro de dossier propre à un programme. Une désignation qui englobe l'ensemble des résidents

- Nos études ont également démontré que le partage d'information entre les PSR de DRHC et les autres programmes fédéraux, provinciaux et territoriaux ne sont pas rares en vertu du cadre législatif en vigueur. En effet, il y a plus de 100 accords fédéraux, provinciaux et territoriaux en place. Le principal identificateur administratif, outre le nom et la date de naissance, utilisé pour faciliter l'appariement des données, est le NAS. Il n'y a aucune coordination centralisée de l'ensemble des accords de concordance des renseignements.

- Des enjeux actuels découlent de l'incapacité d'identifier et d'authentifier les clients au sein des PSR. L'accès à l'Immatriculation aux assurances sociales (IAS) par les provinces et territoires facilitera grandement la vérification de l'identité des personnes qui présentent une demande aux programmes de la sécurité du revenu et aux programmes de soutien du revenu.

- Les processus d'appariement des données en vigueur, qui tournent autour du concept de NAS, satisfont à certaines des exigences des PSR fédéraux, provinciaux et territoriaux. Cependant, un système national spécialement conçu pour atteindre les objectifs de vérification de l'identité et de l'admissibilité et commun à toutes les juridictions des systèmes d'information (SI) pourrait s'avérer plus efficace.

- La plupart des concordances de données actuelles sont de nature réactive, en ce sens qu'elles surviennent après coup. Un processus initial d'appariement de l'information à l'échelle des juridictions permettant de valider l'identité des clients pourrait réduire les paiements injustifiés de prestations dès le départ.

- Tel qu'il a été signalé antérieurement au comité fédéral-provincial-territorial, la plupart des données recueillies étaient de nature qualitative plutôt que quantitative. Très peu de données empiriques ont été obtenues, sans doute à cause du caractère délicat du sujet ou de l'absence de données concrètes. L'analyse des coûts-avantages a été fondée en grande partie sur les preuves qualitatives disponibles.

Conclusions

- À la lumière de l'examen du rapport consolidé qui figure en annexe et des données recueillies à ce jour, on ne peut justifier avec fermeté l'introduction d'un CCI.

- Les recherches effectuées indiquent néanmoins que DRHC pourrait envisager la possibilité de pousser davantage l'utilisation actuelle du NAS afin d'améliorer l'intégrité des programmes, de rehausser la prestation des services et de simplifier l'administration des programmes. Le Ministère pourrait prendre diverses mesures, notamment :

    1. En vertu du cadre existant, optimiser l'IAS en élargissant l'accès aux provinces et territoires dans le but d'améliorer l'authentification de l'identité.

    2. Introduire des mesures préventives et initiales de concordance des données, plutôt qu'un appariement après coup, dans le but de valider l'état des prestations et de prévenir les paiements erronés.

ANNEXE D — DÉVELOPPEMENT DES RESSOURCES HUMAINES CANADA, CODE CLIENT INDIVIDUEL

SOMMAIRE

Historique

- Au cours des deux dernières années, sous les auspices de Développement des ressources humaines Canada (DRHC), les programmes de sécurité du revenu (PSR) fédéraux, provinciaux et territoriaux ont entrepris une étude des avantages et défis liés à l'introduction et à l'utilisation éventuelles d'un code client individuel (CCI) pour les PSR au Canada. Aux fins de la présente étude, un CCI a été défini comme suit : un moyen unique d'identifier une personne dans le cadre d'un dossier administratif. L'objectif de l'étude était de préciser s'il était possible de démontrer qu'un CCI pourrait :
    - maintenir ou améliorer le respect de la vie privée et de la confidentialité;
    - rehausser la prestation des services;
    - simplifier l'administration des programmes;
    - améliorer l'intégrité des programmes.
- Aux fins de cette étude, les scénarios envisagés en matière d'utilisation d'un CCI comprenaient ce qui suit :
    - le statu quo, c.-à-d. le numéro d'assurance sociale (NAS) actuel;
    - un NAS « modifié »;
    - un nouveau numéro.

Situation actuelle

- Nos recherches ont révélé que les juridictions de la sécurité du revenu provinciales et territoriales utilisent déjà le NAS comme identificateur administratif pour leurs clients de la sécurité du revenu. En fait, de 90 à 100 p. 100 (selon la juridiction) des clients des programmes de la sécurité du revenu provinciaux et territoriaux disposent d'un NAS.

- Le modèle de mesure du rendement actuellement utilisé par le Ministère fait en sorte que les enquêteurs de l'assurance-emploi n'accordent qu'une très faible priorité aux enquêtes sur le NAS.
- La diminution du nombre et de la qualité des enquêtes sur le NAS peut aussi miner l'intégrité de la base de données du NAS.

Carte d'assurance sociale

1. Des milliers de personnes qui n'ont pas de statut juridique au Canada sont titulaires de NAS valides :
   - Depuis 1976, année où l'on a commencé à utiliser la série 900, 1 242 000 NAS temporaires ont été attribués. En 1998, quelque 680 000 NAS temporaires restent actifs et 66 p. 100 de ceux-ci datent de plus de cinq ans, soit une longue période pour un numéro considéré comme temporaire.
   - L'écart pourrait être attribuable à des titulaires de NAS qui résident au Canada illégalement.
2. La carte d'assurance sociale n'a pas été conçue pour identifier son titulaire. Par conséquent, elle ne comporte aucune caractéristique de sécurité qui la rattache à celui-ci (photographie, description, etc.) pouvant servir à prévenir et à empêcher la falsification et l'utilisation inappropriée de la carte.

Peines relatives au NAS

Les peines découlant des enquêtes fructueuses sur le NAS sont minimes :

- La *Loi sur l'assurance-emploi* stipule que la peine relative à toute infraction concernant le NAS est une amende inférieure ou égale à 1 000 $ ou l'emprisonnement d'une durée maximale d'un an, ou ces deux sanctions. Des accusations en vertu du *Code criminel* peuvent aussi être portées.
- Très peu de fraudeurs se font prendre et même si quelqu'un est pris, le Ministère porte rarement des accusations criminelles.
- Des amendes si faibles ne semblent pas justifier le temps et les efforts considérables qu'exige une poursuite et leur effet dissuasif est douteux. Ainsi, il n'existe en fait aucune peine pour des activités susceptibles de causer un tort considérable aux programmes sociaux, à la perception des impôts, aux activités commerciales de même qu'à la protection des renseignements personnels et à la sécurité des Canadiens.

Enquêtes relatives au NAS

1. On ne consacre que peu d'efforts aux enquêtes sur le NAS :
    - Étant donné que DRHC est responsable du contrôle du NAS, il est d'une importance vitale qu'il mène des enquêtes proactives et efficaces pour prévenir, déceler et empêcher les abus qui pourraient coûter plusieurs millions de dollars aux contribuables et causer des préjudices.
    - L'usurpation d'identité — l'utilisation illégale des renseignements d'identité d'une personne, y compris le NAS — est un phénomène croissant en Amérique du Nord.
    - Le nombre déjà restreint d'enquêtes continue de diminuer.
    - La Direction générale des Programmes de la sécurité du revenu a effectué encore moins d'enquêtes relatives au NAS que les enquêteurs de l'assurance-emploi.
2. Les enquêtes sur le NAS pourraient donner des résultats substantiels :
    - Il existe de nombreux types d'abus sur l'utilisation du NAS qui conduisent à des enquêtes. Ces abus sont signalés par Revenu Canada, l'Assurance-emploi, le Régime de pensions du Canada, la Sécurité de la vieillesse et les provinces. D'autres sont signalés par des institutions financières.
3. La qualité des enquêtes sur le NAS a besoin d'être améliorée :
    - Selon l'estimation du VG, moins de 1 p. 100 des enquêtes finissent par produire un dossier assez solide pour porter des accusations.
4. Les indicateurs de rendement existants dissuadent les fonctionnaires d'effectuer des enquêtes sur le NAS :
    - Les économies pour les autres programmes qui découlent des enquêtes sur le NAS ne sont pas attribuées par DRHC aux enquêteurs de l'assurance-emploi.

- Le paragraphe 6(2) de la *Loi sur la protection des renseignements personnels* oblige les institutions gouvernementales à veiller, dans la mesure du possible, à ce que les renseignements personnels utilisés à des fins administratives soient exacts, complets et à jour.

Preuve d'identité

1. Il faut appliquer une plus grande rigueur dans le programme de preuve d'identité :

   - D'une façon générale, la procédure de demande de NAS n'exige qu'un seul document d'identité et ne comporte pas d'autres moyens de confirmer l'identité, comme d'autres programmes de DRHC et du Bureau des passeports.

   - En général, les demandes reçues par la poste représentent un risque un peu plus grand que les demandes présentées en personne, parce qu'on accepte des photocopies certifiées — qui elles-mêmes pourraient avoir été certifiées frauduleusement — et que les demandeurs qui éveillent des soupçons ne peuvent pas être interrogés.

   - Environ 20 p. 100 du nombre total de cartes de NAS produites chaque année sont délivrées pour remplacer des cartes dont les titulaires ont signalé la perte, le vol ou la détérioration. Les contrôles relatifs à cette activité ont besoin d'être améliorés.

2. Le fait de se fier surtout aux certificats de naissance comme fondement de l'identité comporte des inconvénients importants. Le certificat de naissance présente certaines lacunes :

   - Il est relativement facile à contrefaire.

   - Comme il est sur support papier, il se détériore rapidement, ce qui rend l'information plus difficile à vérifier.

   - Il n'existe aucune caractéristique de sécurité établissant un lien entre le certificat et son titulaire.

   - Le recours généralisé aux documents délivrés par divers organismes crée une situation d'interdépendance. Toutes les parties deviennent ainsi plus vulnérables.

   - Dans le cas du NAS, la mesure dans laquelle le document d'identité est vérifié dépend de la capacité des commis et des agents de DRHC à reconnaître les documents frauduleux ou falsifiés.

   - Les modifications de la conception des documents, l'absence de photographie, la mobilité des personnes qui peuvent transporter des documents d'identité produits par de nombreuses administrations différentes, tout cela rend de plus en plus difficile pour les employés du programme qui étudient les documents de cerner les falsifications ou les renseignements modifiés.

   - On n'attribue pas de cote à la fiabilité des documents et, par conséquent, l'approche de DRHC n'est pas adaptée à la qualité des documents d'identité fournis par les organismes émetteurs.

□ mai 1999	Dépôt des rapports sur les enquêtes et les sanctions devant le comité directeur du projet
□ été 1999	Examen des rapports provisoires sur l'intégrité des données, le PPI et la carte d'assurance sociale
□ été 1999	Dépôt des rapports sur l'intégrité des données, le PPI et la carte d'assurance sociale devant le comité directeur du projet pour décision

Annexe A — Observations tirées du rapport du vérificateur général

Intégrité des données

1. Il existe un écart important entre le nombre de titulaires de NAS et la taille de la population canadienne, un écart d'environ 3,8 millions pour les personnes de 20 ans ou plus :
   - Le nombre de décès non inscrits est un des facteurs les plus importants de l'écart.
   - Le nombre de Canadiens vivants inscrits dans la base de données du NAS en 1998 reste beaucoup plus élevé que le nombre indiqué dans les données de Statistique Canada.
   - Sans des efforts supplémentaires pour inscrire les décès, les écarts continueront de s'élargir en même temps que les possibilités de confusion et d'inefficience et le risque que les identités des personnes décédées soient utilisées pour des activités frauduleuses.
2. Les sources d'information existantes ne sont pas exploitées à fond et on pourrait faire davantage pour établir de nouvelles sources :
   - La comparaison de données avec les provinces, les territoires et les gouvernements étrangers ouvre l'accès à d'autres sources de renseignements qui pourraient permettre de détecter des centaines de milliers de décès non déclarés.
   - Même si le RPC, Revenu Canada et le RAS partagent davantage de données, le problème du rapprochement entre les différentes sources reste entier. Par exemple, Revenu Canada ne fournit pas au RAS les corrections qu'il apporte aux fichiers des contribuables lorsqu'il remarque des différences dans la date de naissance, le nom, etc.
3. Il existe des millions de NAS dont l'identité du titulaire n'a pas été certifiée. Il y a dans le RAS quelque 11,8 millions de comptes qui, en raison des possibilités d'erreurs, de mauvaises utilisations et d'abus, pourraient être une grande source de préoccupations pour les organismes qui utilisent beaucoup le NAS.
4. Les renseignements concernant la naissance ne sont pas faciles à vérifier auprès des organisations qui les délivrent :
   - Les préposés au RAS ne vérifient pas habituellement, auprès des organisations qui les délivrent, la validité des renseignements inscrits sur les documents acceptés pour les demandes de NAS.

- **Échéances :**

□ novembre 1998	Équipe de projet complète
□ novembre 1998	Première ébauche du mandat
□ décembre 1998	Consultation de Citoyenneté et Immigration
□ janvier 1999	Consultations d'utilisateurs de NAS autorisés
□ février 1999	Consultations des partenaires (p. ex. les provinces)
□ mars 1999	Consultations des employeurs, des groupes d'intérêt, des promoteurs des droits de la personne et des droits à la protection des renseignements personnels Consultations du groupe des Systèmes de DRHC
□ avril 1999	Première ébauche du rapport

Coordination du projet

- **Mandat :** Coordonner les activités des cinq groupes de travail pour en assurer la cohérence et l'efficience. Élaborer une approche ou un plan global pour la gestion des questions administratives liées au NAS.
- **Composition :** Cinq présidents des groupes de travail; participants choisis au sein d'autres ministères (RC, CT).
- **Moyens :** Rencontres multilatérales entre DRHC, les provinces et les autres ministères; rencontres de SMA et de SM de DRHC et des autres ministères.
- **Résultat :** Plan et stratégie de consultation auprès des provinces avec la participation des ministères responsables des services sociaux, approche coordonnée et gestion horizontale des dossiers .
- **Échéances :**

□ août 1998	Présentation aux directeurs provinciaux et territoriaux responsables de la technologie de l'information
□ septembre 1998	Présentation aux directeurs F-P-T responsables des services sociaux
□ décembre 1998	Rencontre interministérielle des SMA suivie d'une rencontre des SM
□ janv.- mars 1999	Négociations du protocole d'entente avec Développement des ressources humaines — Nouveau-Brunswick
□ printemps 1999	Discussions avec les fonctionnaires et les sous-ministres responsables des services sociaux, des statistiques de l'état civil et de la protection des renseignements personnels
□ mars 1999	Examen du rapport provisoire sur les enquêtes relatives au NAS
□ avril 1999	Examen du rapport provisoire sur les sanctions relatives au NAS

- **Moyens :** Trouver des solutions de rechange au système actuel et formuler des recommandations au Comité de gestion.
- **Résultats possibles :**

  6. Meilleure information du public.
  7. Le Conseil du Trésor reconnaît l'importance des enquêtes touchant le NAS.
  8. Plus d'agents affectés aux enquêtes sur le NAS.

- **Échéances :**

□ novembre 1998	Équipe de projet complète
□ novembre 1998	Première ébauche du mandat
□ décembre 1998	Mise sur pied de l'unité de contrôle des enquêtes sur le NAS
□ janvier 1999	Lettre aux régions soulignant l'importance des lettres d'attestation
□ février 1999	Consultation et analyse
□ mars 1999	Première ébauche du rapport
□ mars 1999	Mise en oeuvre de pratiques exemplaires donnant lieu à des poursuites dont les résultats nous sont favorables

Groupe de travail nº 5 : Carte d'assurance sociale

- **Mandat :** Examiner la possibilité de mettre une date d'expiration sur les cartes d'assurance sociale temporaires et d'ajouter de nouveaux dispositifs de sécurité.
- **Composition :** DRHC : Assurance (responsable), Services nationaux, Sécurité du revenu, Enquêtes et contrôle; Revenu Canada et Citoyenneté et Immigration.
- **Moyens :**

  □ Déterminer l'ampleur de la situation.
  □ Consultations et partenariats.
  □ Analyse d'impact.
  □ Stratégie de mise en oeuvre.

- **Résultats possibles :**

  □ Aucune modification de la carte d'assurance sociale — confirmer que c'est un dossier administratif.
  □ Mettre une date d'expiration sur les cartes temporaires uniquement.
  □ Émission d'une carte à puce.
  □ Dépendra de la décision du gouvernement concernant l'avenir du NAS.

- mars 1999 — Révision du manuel des NAS et élaboration de plans pour la mise en oeuvre sur l'intranet
- juin 1999 — Première ébauche du rapport

Groupe de travail nº 3 : Pénalités

- **Mandat :** Examiner la meilleure façon d'empêcher l'utilisation frauduleuse du NAS, y compris la possibilité d'infliger des sanctions administratives en cas d'infractions. Il n'existe actuellement aucune sanction sauf pour les fraudes touchant d'autres programmes (AE, Sécurité du revenu, Revenu Canada, etc.).
- **Composition :** DRHC : Enquêtes et contrôle (responsable), Admissibilité aux prestations, Services d'assurance, Services juridiques et Finances.
- **Moyens :** Déterminer des options pour empêcher l'utilisation frauduleuse du NAS; examiner des changements législatifs possibles pour contrer les fraudes, dont les recommandations initiales, et en tenant compte des implications juridiques, de la Charte et de la protection des renseignements personnels. Consulter les régions sur les répercussions possibles.
- **Résultats possibles :**
  3. Aucun changement.
  4. Meilleure information du public.
  5. Application de sanction comme pour l'AE.
- **Échéances :**
  - novembre 1998 — Équipe de projet complète
  - novembre 1998 — Première ébauche du mandat
  - décembre 1998 — Consultations — AC
  - février 1999 — Consultations — régions
  - mars 1999 — Consultations sur la formulation des dispositions législatives
  - avril 1999 — Présentation à la Commission
  - À déterminer — Décision sur l'échéancier d'adoption des dispositions législatives

Groupe de travail nº 4 : Enquêtes

- **Mandat :** Examiner la meilleure façon d'empêcher l'utilisation frauduleuse du NAS; envisager la modification des indicateurs de rendement d'Enquêtes et contrôle pour améliorer la qualité des enquêtes liées au NAS et en augmenter le nombre.
- **Composition :** DRHC : Enquêtes et contrôle (responsable); consultations avec le Conseil du Trésor, Revenu Canada et d'autres ministères et organismes susceptibles de s'intéresser à la question des fraudes liées au NAS.

- □ avril 1999 — Recensement des sources de données supplémentaires sur les naissances et les décès
- □ avril 1999 — Stratégie de mise en oeuvre pour l'obtention de données supplémentaires sur les naissances et les décès
- □ mai 1999 — Traitement des comptes non certifiés en suspens
- □ mai 1999 — Adjonction des données sur les décès de la SV à partir des dossiers archivés
- □ mai 1999 — Détermination de l'activité relative aux NAS à partir des dossiers archivés de la SV
- □ juin 1999 — Première ébauche du rapport

Groupe de travail nº 2 : Preuve de l'identité

- **Mandat :** Examiner le processus de vérification de l'identité utilisé lors du traitement des demandes de NAS. Jusqu'en 1976, aucune preuve d'identité n'était exigée puisque le NAS était considéré comme un simple numéro d'identification de dossier.
- **Composition :** DRHC : Services nationaux (responsable), Services d'assurance, Enquêtes et contrôle, Sécurité du revenu; Citoyenneté et Immigration et Revenu Canada.
- **Moyens :**
  - □ Examen des principaux documents exigés à l'appui de la demande de NAS.
  - □ Examen des procédures de traitement des demandes de NAS.
  - □ Examen des procédures utilisées dans d'autres programmes et d'autres instances administratives pour la vérification de l'identité.
  - □ Recommandation d'une nouvelle preuve d'identité.
  - □ Mise en place de mécanismes de contrôle plus stricts.
- **Résultats possibles :**

  1. Preuves d'identité supplémentaires exigées à l'appui de la demande.

  2. Vérification des documents à la source, p. ex. lien avec les statistiques de l'état civil de la province afin de vérifier les données sur la naissance.
- **Échéances :**
  - □ novembre 1998 — Équipe de projet complète
  - □ novembre 1998 — Première ébauche du mandat
  - □ décembre 1999 — Mise en oeuvre de procédures pour repérer les identités frauduleuses
  - □ janvier 1999 — Examen des documents d'identité utilisés dans d'autres programmes
  - □ avril 1999 — Consultation des provinces et territoires et analyses

- Assurer une meilleure protection de la carte d'assurance sociale si le gouvernement décide d'adopter un code d'identification personnel.

Plan de travail de DRHC

Conscient de ses responsabilités touchant l'émission de NAS, le maintien du Registre d'assurance sociale et les enquêtes sur les abus présumés, DRHC a élaboré un plan d'action qui s'articule autour de cinq groupes de travail :

Groupe de travail nº 1 : Intégrité des données

- **Mandat :** Améliorer l'intégrité des données figurant dans le Registre d'assurance sociale. Les décès et les départs du pays n'y sont pas tous consignés.
- **Composition :** DRHC : Services nationaux (responsable), Services d'assurance, Systèmes, Sécurité du revenu, Enquêtes et contrôle et Revenu Canada.
- **Moyens :**
  - Réduire le nombre de comptes non certifiés par l'accès à d'autres programmes exigeant une preuve d'identité.
  - Annoter les NAS «inutilisés», p. ex. aucune transaction à RC, au RPC, à l'AE.
  - Augmenter le nombre de décès consignés par l'accès aux données des provinces, à Statistique Canada, aux Affaires étrangères, etc.
- **Résultats possibles :**
  - Protocoles d'ententes et accords permettant l'accès à d'autres bases de données fédérales ou provinciales sur les naissances, les décès et les changements de nom.
  - Couplage de données pour éliminer l'arriéré de données sur les décès.
  - Accès aux données de l'AE, de la Sécurité du revenu et de Revenu Canada pour déterminer si le NAS est actif.
- **Échéances :**

novembre 1998	L'équipe de projet est complète
novembre 1998	Première ébauche du mandat
décembre 1998	Délimitation du contenu de la base de données NAS Lettre à Statistique Canada pour demander les données sur les décès
mars 1999	Adjonction des données sur les décès de la SV à partir de la base de données actives
mars 1999	Détermination de l'activité relative aux NAS à partir de la base de données actives de la SV
mars 1999	Fichier de tous les NAS actifs de Revenu Canada sur la base de données d'identification

□ mars 1999	Fichier de tous les NAS actifs de Revenu Canada sur la base de données d'identification
□ mai 1999	Adjonction des données sur la mortalité de la SV et des données certifiées à partir des dossiers archivés
□ mai 1999	Détermination de l'activité relative aux NAS à partir des dossiers archivés de la SV

Principales questions administratives soulevées par le vérificateur général

- Développement des ressources humaines Canada administre le NAS dans l'esprit du cadre juridique selon lequel le NAS devrait être un code d'identification de dossier (numéro de compte) pour certains programmes du gouvernement fédéral. Cependant, le public perçoit souvent le NAS comme un code d'identification personnel ou même une carte d'identité.
- L'utilisation du NAS hors du domaine fédéral a dépassé l'esprit de la politique du Conseil du Trésor établie en 1989, laquelle visait à empêcher ce numéro de devenir un code d'identification personnel national. Au cours de sa vérification, le vérificateur général a constaté que le NAS est devenu un code d'identification numérique commun, tant à l'intérieur qu'à l'extérieur du gouvernement fédéral, pour un large éventail de prestations et de transactions relatives au revenu, entre autres utilisations.
- Toutefois, le programme du NAS comporte un certain nombre de lacunes en ce qui concerne l'intégrité des données, la preuve de l'identité, les sanctions, les enquêtes et la carte (pour plus de détails, voir l'annexe A, «Observations tirées du rapport du vérificateur général»). Avec l'utilisation accrue du NAS, ces lacunes sont devenues plus importantes.

Réponse de DRHC : Principaux défis

DRHC a cerné cinq grandes tâches d'ordre administratif à accomplir pour donner suite au rapport du vérificateur général, à savoir :

1. Se pencher sur les questions entourant l'intégrité des données figurant dans le Registre d'assurance sociale.
2. Examiner le Programme de preuve de l'identité et son champ d'application.
3. Déterminer la meilleure façon d'améliorer la qualité des enquêtes sur le NAS et d'en accroître le nombre.
4. Déterminer des moyens de réprimer plus efficacement les fraudes touchant le NAS, y compris les sanctions administratives.
5. Explorer les changements possibles relativement à la carte d'assurance sociale :

   - Fixer une date d'expiration pour les NAS temporaires

Introduction

Dans le présent document sont exposés les principaux éléments d'un plan de travail visant à améliorer la gestion du NAS, en réponse au rapport du vérificateur général.

Contexte

Évolution du NAS

Le numéro d'assurance sociale a été adopté en 1964, comme moyen de fournir un numéro de dossier aux clients de l'assurance-chômage, du Régime de pensions du Canada et du Régime de rentes du Québec. En 1967, il est aussi devenu un code d'identification de dossier pour Revenu Canada. En 1976, on a établi le Programme de preuve de l'identité afin de vérifier l'identité et la situation au Canada des personnes demandant un NAS. On voulait ainsi empêcher que plus d'un NAS soit attribué à une même personne et préserver l'intégrité du Registre d'assurance sociale.

Rôles et responsabilités touchant le NAS

- **DRHC** est responsable de la gestion du NAS; il émet les numéros, maintient la base de données des NAS, enquête sur les abus et prend les règlements nécessaires.
- Le **Conseil du Trésor** est responsable de la politique et des lignes directrices régissant la collecte et l'utilisation des NAS au palier fédéral.
- Le **commissaire à la protection de la vie privée** enquête sur les plaintes concernant le NAS.
- Le **ministère de la Justice** aide les autres ministères à fournir des avis juridiques liés au NAS en application de la *Loi sur la protection des renseignements personnels* et à répondre à des demandes de renseignements de nature générale sur l'utilisation du NAS par le secteur privé.

Rapport du vérificateur général

En 1998, le bureau du vérificateur général du Canada a procédé à un examen approfondi de la gestion du numéro d'assurance sociale. Les conclusions de cette vérification se trouvent dans le chapitre 16 du rapport déposé par le vérificateur général le 29 septembre 1998.

DRHC est chargé au premier plan de corriger les lacunes administratives relevées dans la gestion du NAS; avec l'aide des Programmes de la sécurité du revenu, de Statistique Canada et de Revenu Canada, il a défini plusieurs mesures à court terme :

□ février 1999	Rencontre du sous-ministre adjoint avec ses homologues des Services sociaux et de Statistique
□ mars 1999	Adjonction des données sur la mortalité de la SV et des données certifiées à partir de la base de données actives

ÉBAUCHE

DÉVELOPPEMENT DES RESSOURCES HUMAINES CANADA

RÉPONSE AU RAPPORT DU VÉRIFICATEUR GÉNÉRAL

PLAN DE TRAVAIL 1998-1999 VISANT À AMÉLIORER LA GESTION DU NUMÉRO D'ASSURANCE SOCIALE (NAS)

Programmes

1. Programmes sur le revenu et sur les soins de santé (Anciens Combattants Canada)
2. Programme d'aide à l'adaptation des immigrants (Citoyenneté et Immigration Canada)
3. Office d'aide à l'adaptation des travailleurs (Développement des ressources humaines Canada)
4. Fichier dosimétrique national en ce qui concerne les radioexpositions professionnelles (Santé Canada)
5. Programme de logement pour les ruraux et les Autochtones (Société canadienne d'hypothèques et de logement)
6. Programme en matière d'assistance et de développement économique (Affaires indiennes et du Nord Canada)
7. Appels en matière d'impôt sur le revenu et décisions défavorables (Revenu Canada)

Source : ministère de la Justice et Secrétariat du Conseil du Trésor, juin 1998

ANNEXE B
Utilisations autorisées du numéro d'assurance sociale (NAS) (Pièce 16.1 du rapport du vérificateur général)

Lois et règlements

1. *Loi d'exécution du budget* (Subvention canadienne pour l'épargne-études)
2. *Loi électorale du Canada*
3. *Règlement du Canada sur les normes du travail* (*Code canadien du travail*)
4. *Règlement sur le Régime de pensions du Canada* (*Régime de pensions du Canada*)
5. *Loi fédérale sur l'aide financière aux étudiants*
6. *Règlement fédéral sur les prêts aux étudiants* (*Loi fédérale sur les prêts aux étudiants*)
7. *Loi sur la Commission canadienne du blé*
8. *Loi sur l'assurance-emploi*
9. *Loi sur la taxe d'accise* (partie IX)
10. *Règlement sur la saisie-arrêt* (*Loi d'aide à l'exécution des ordonnances et des ententes familiales*)
11. *Loi sur la protection du revenu agricole*
12. *Règlement sur les demandes de versement au titre de la taxe d'accise sur l'essence et l'essence d'aviation* (*Loi sur la taxe d'accise*)
13. *Loi de l'impôt sur le revenu*
14. *Loi sur les prestations d'adaptation pour les travailleurs*
15. *Règlement sur la sécurité de la vieillesse* (*Loi sur la sécurité de la vieillesse*)
16. *Règlement concernant la Loi sur la cession du droit au remboursement en matière d'impôt* (*Loi sur la cession du droit au remboursement en matière d'impôt*)
17. *Règlement sur les allocations aux anciens combattants* (*Loi sur les allocations aux anciens combattants*)

Organismes et particuliers	Date	Fascicule
Commissaire à l'information et à la vie privée	Le 3 février 1999	47
Ann Cavoukian, commissaire à l'information et à la protection de la vie privée		
David Flaherty, commissaire à l'information et à la protection de la vie privée		
Action/réseau consommateurs	Le 10 février 1999	48
Marie Vallée, analyste, Politique et réglementation, Télécommunications		
Centre de bioéthique, Institut de recherches cliniques de Montréal		
Pierrot Péladeau, coordonnateur scientifique, Programme éthique et télésanté		
Association des banquiers canadiens		
Linda Routledge, directeur		
Ted Rowan-Legg, conseiller général adjoint		
Richard Rudderham, vice-président		
Revenu Canada		
Kathy Turner, directeur général		
Gendarmerie royale du Canada		
Victor Gareau, sergent d'état major		
Développement des ressources humaines Canada	Le 3 mars 1999	49
Jacques Bourdages, directeur délégué, Service national		
Dennis Kealey, directeur général		
John Knubley, sous-ministre adjoint de l'Assurance		
Doug Matheson, directeur général, Service d'assurance		
« Ibis Research Inc. »	Le 9 mars 1999	50
Alan Breakspear, président		
« Signals 9 Solutions »		
Philip Attfield , président		

ANNEXE A
Liste des témoins

Organismes et particuliers	Date	Fascicule
Bureau du vérificateur général du Canada	Le 4 novembre 1998	43
L. Denis Desautels, vérificateur général du Canada		
Maurice Laplante, directeur		
David Rattray, vérificateur général adjoint		
Ministère de la Justice	Le 26 novembre 1998	45
Lita Cyr, conseillère juridique		
Brian Jarvis, conseiller juridique		
Développement des ressources humaines Canada		
Jacques Bourdages, directeur délégué, Service national		
Hy Braiter, sous-ministre adjoint principal		
Bob Nichols, directeur		
Bureau du commissaire à la protection de la vie privée du Canada		
Julien Delisle, directeur exécutif		
Bruce Phillips, commissaire à la protection de la vie privée du Canada		
Conseil du Trésor du Canada		
Ross Hodgins, agent supérieur de politique		
Ian Sinclair, directeur, Division des politiques de l'information		
« Advanced Card Technology Association of Canada »	Le 3 février 1999	47
Catherine Johnston, présidente/directrice générale		
Ville de Toronto		
Rita Reynolds, directeur « Corporate Access and Privacy Office »		
Association des consommateurs du Canada		
Jim Savary, professeur		

- Comment faire pour empêcher les comparaisons inappropriées de données?
- Quelles sont les meilleures façons de protéger les citoyens de l'incidence croissante de vol d'identité?
- Serons-nous prêts à satisfaire ceux qui, à mesure que le commerce électronique se répand, réclament pour chaque Canadien un identificateur sûr?
- À mesure que la technologie se raffine et prend plus d'ampleur, faudrait-il accroître les pouvoirs du Commissaire fédéral à la protection de la vie privée pour lutter contre les intrusions dans la vie privée des Canadiens et, le cas échéant, quelle serait la portée de ces pouvoirs?
- Quels coûts la protection de la vie privée entraînerait-elle?
- Dans quelle mesure les Canadiens sont-ils disposés à faire les frais d'une technologie coûteuse pour assurer la protection de leur vie privée?
- Comment équilibrons-nous le besoin d'accroître l'efficacité et les droits de chacun à la protection de la vie privée?
- Comment parons-nous, de façon proactive, à la fraude et aux abus du système de NAS ainsi qu'aux autres formes de fraude relatives aux cartes?

Voilà un échantillon des grandes questions d'orientation auxquelles les gouvernements devront trouver réponse dans les années à venir. Impossible de répondre par oui ou non, ou par vrai ou faux, à aucune d'elles. Chacune suppose des compromis. Comme dans le débat public de portée générale sur la vie privée, les décisions fondamentales reposent ici sur un « consentement éclairé ». Pour prendre ces décisions, les politiciens et les Canadiens ont besoin de se renseigner et de discuter. Les décisions sur l'utilisation actuelle du NAS ont été trop souvent prises par défaut; c'est une chose que, inacceptable alors comme aujourd'hui, il faudrait éviter à l'avenir.

Il serait encore ici très tentant de détourner un système remanié de NAS ou une nouvelle carte de son objet initial. La dérive de la finalité, aiguillonnée par le besoin d'« efficacité », est un puissant argument. Sur le plan individuel, les citoyens ne comprennent pas bien ce qu'ils abandonnent. Le récent procès intenté, et gagné, par le commissaire à la protection de la vie privée pour empêcher la comparaison de données recueillies lorsque les Canadiens entrent ou sortent du pays aux demandes d'allocation d'assurance-chômage en a révélé des exemples. Compte tenu de ces considérations, le Comité recommande :

16. Que DRHC produise d'ici au 31 décembre 1999, un rapport exposant une série d'options, assorties de leur coût, pour améliorer le système de NAS ou le remplacer par un tout nouveau système de cartes. Ce rapport devrait évaluer la possibilité d'adopter au Canada un modèle administratif de NAS semblable au modèle de la banque Carrefour Belge (annexe D du présent rapport).

L'étude du NAS réalisée par le Comité a fait ressortir les inquiétudes globales qu'inspirent la technologie, la protection de la vie privée et la comparaison des données. Les témoins n'ont cessé, tout au long des audiences sur le NAS, de soulever ces grandes questions. Dans son rapport *La vie privée : où se situe la frontière?* déposé en avril 1997, l'ancien Comité permanent des droits de la personne et de la situation des personnes handicapées de la Chambre des communes traitait longuement et en profondeur de ces considérations de politique gouvernementale. L'aboutissement d'une étude intensive des incidences de l'évolution technologique sur les droits de la personne et de la protection de la vie privée, ce rapport amplifie et explique bon nombre d'inquiétudes que les membres du Comité ont commencé à ressentir, à mesure qu'ils examinaient la question plus restreinte de l'avenir du système de NAS.

De l'avis du Comité, le rapport intitulé *La vie privée : où se situe la frontière?* recense, examine, évalue et recommande des moyens de parer à ces questions, et ce dans un cadre mis au point au cours d'un très vaste processus de consultations et de débats publics. Étant donné la date à laquelle le rapport a été déposé, le gouvernement n'y a pas réagi. Par conséquent, le Comité :

17. Dans le respect de la législation existante, adopte les recommandations et prend acte des opinions dissidentes formulées dans le troisième rapport du Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes intitulé *La vie privée : où se situe la frontière?* déposé à la Chambre des communes le 27 avril 1997 (annexe E du présent rapport). Il sollicite, conformément à l'article 109 du Règlement, une réponse à ces recommandations.

En conclusion, le Comité se retrouve ainsi devant une série de questions qu'il n'a pas eu le temps d'examiner comme il l'aurait souhaité.

- Comment les droits des citoyens à la vie privée seront-ils protégés si le NAS est « modernisé » ou « remplacé »?

PARTIE 3 — L'AVENIR DU SYSTÈME DE NUMÉROS D'ASSURANCE SOCIALE : CONSIDÉRATIONS STRATÉGIQUES

Le Comité a signalé, au début du présent rapport, que ses audiences sur le système de numéros d'assurance sociale ont soulevé plus de questions qu'elles n'ont permis d'en régler. Il s'est constamment heurté, tout au long de ses travaux, à la réalisation que la solution aux problèmes administratifs immédiats (abordés à la partie 2) dont le rapport du vérificateur général fait état ne s'attaque pas au problème central et fondamental du contexte dans lequel le système de NAS est utilisé. Nous n'avons pas tardé à comprendre que notre travail, en tant que parlementaires, consistait à déterminer dans quelle mesure le système a évolué et s'est éloigné du but initial. À maintes reprises, divers témoins ont réitéré l'importance fondamentale de clarifier l'objet du NAS.

Le débat élargi sur les politiques gouvernementales devrait donc viser à répondre aux questions suivantes :

1. Faudrait-il revenir au but initial du NAS, qui était de servir de numéro d'identification des dossiers des programmes gouvernementaux? Si oui, serait-il possible de récupérer le système en donnant suite aux recommandations formulées ci-desssus ou devrait-on faire table rase et le remplacer par une nouvelle carte, comme une carte du millénaire fondée sur la technologie de pointe des « cartes à mémoire » munies d'une puce informatique, ou par un identificateur biométrique?

2. Le moment est-il venu de reconnaître ce à quoi le NAS sert en réalité et de prendre des mesures pour le convertir en numéro personnel d'identification de chaque résident du Canada? L'adoption d'une telle carte peut-elle s'accompagner, pour protéger la vie privée de chacun, du recours au cryptage et à d'autres possibilités qu'offre la carte à puce?

Le Comité abonde vivement dans le sens de ce que certains témoins lui ont dit, à savoir que toute tentative de transformer le NAS en numéro national d'identification doit s'accompagner d'un vaste débat politique et d'un apport adéquat et approprié du grand public. La création d'un système national d'identification présente des problèmes de protection de la vie privée qu'il faut résoudre. La vie privée est trop fragile et les moyens d'en garantir la protection trop faibles, et susceptibles de le rester. Il faudrait compenser par des moyens techniques et légaux adéquats de sauvegarde la très forte tentation, autant pour le secteur public que privé, d'utiliser les données de tout système national d'identification à d'autres fins ou sans autorisation.

Nous croyons cependant nécessaire de donner aux citoyens l'occasion de peser les coûts et avantages de tout changement notable du NAS ou de son successeur, et d'en débattre publiquement.

Compte tenu des coûts imputables à l'utilisation frauduleuse du NAS, le gouvernement fédéral, et en particulier DRHC, doivent se concentrer davantage sur les enquêtes touchant les cas de fraudes possibles. À l'instar du vérificateur général, nous croyons que ces enquêtes se situent très bas dans la liste de priorités de DRHC. Il faut corriger la situation. Une façon d'y arriver serait de mieux mesurer le rendement. À notre avis, le système actuel de mesure du rendement de DRHC n'est pas approprié. Il met l'accent par exemple sur les économies que permettent de réaliser les enquêtes sur les fraudes et les abus touchant l'assurance-emploi. Toute mesure prise doit tenir compte du fait que l'utilisation frauduleuse des cartes de numéro d'assurance sociale affecte l'ensemble des programmes gouvernementaux dans le cadre desquels on se sert du NAS comme numéro de dossier (voir l'annexe B). Par conséquent, nous recommandons :

12. **Que DRHC instaure un nouveau mécanisme de mesure du rendement montrant les économies globales que la lutte contre l'utilisation frauduleuse des cartes du numéro d'assurance sociale permet de réaliser. L'analyse de rentabilisation concernant ce nouveau mécanisme de mesure du rendement devrait être soumise au Conseil du Trésor lors de la prochaine série de présentations.**

13. **Que selon les résultats que produira le nouveau mécanisme de mesure, DRHC affecte les ressources humaines appropriées pour réaliser les enquêtes au sujet de l'utilisation frauduleuse d'un numéro d'assurance sociale.**

14. **Que dans son prochain rapport de rendement annuel au Parlement, et dans ses rapports ultérieurs, DRHC réserve une section à la gestion du numéro d'assurance sociale et du Registre d'assurance sociale.**

Nos recommandations recoupent jusqu'ici celles du vérificateur général et du Comité des comptes publics, en particulier en ce qui concerne les problèmes à court terme et immédiats touchant l'administration du système de NAS. Nous désirons que les réponses qui feront suite à nos recommandations tiennent compte du consensus qui s'est dégagé dans ce dossier du côté des trois instances parlementaires. Les mesures correctives nécessaires doivent être prises sans tarder.

15. **Que DRHC présente au Parlement, d'ici le 30 septembre 1999, un rapport d'étape sur la mise en oeuvre du plan de travail 1998-1999 pour améliorer l'administration du NAS (annexe C du présent rapport).**

d'un numéro). Nous ajoutons toutefois une mise en garde. Certes, nous croyons qu'étendre ce genre de système d'identification à d'autres régions pourrait aider à garantir l'exactitude des données du RAS et à empêcher l'émission de nouvelles cartes d'assurance sociale en faveur de fraudeurs. Néanmoins, la province où le projet pilote fut réalisé ne dispose d'aucune loi sur la protection des renseignements personnels. Après avoir revu les données compilées par le groupe n° 2 sur la preuve d'identité[10], nous recommandons :

8. **Que DRHC agisse sans tarder pour rendre prioritaires les questions touchant la protection des renseignements personnels et transmette les rapports du Groupe de travail sur la preuve d'identité et de *tous* les groupes de travail mentionnés dans l'ébauche de plan de travail pour améliorer l'administration du NAS au commissaire à la protection de la vie privée du Canada pour obtenir ses commentaires.**

9. **Que DRHC publie un rapport d'évaluation du projet pilote mené au Nouveau-Brunswick et qu'il le présente au commissaire à la protection de la vie privée du Canada d'ici le 30 septembre 1999. Ce dernier devrait présenter ses commentaires sur le rapport d'évaluation au Comité au plus tard dans les 30 jours qui suivent.**

10. **Que DRHC veille à ce que tous les nouveaux programmes ou procédures mis de l'avant pour garantir la validité des documents concernant la preuve d'identité soient restreints à l'information vraiment nécessaire afin de vérifier la validité des documents.**

Lors de nos réunions au sujet du système du NAS, nous avons entendu des témoignages — dont certains stupéfiants — au sujet de l'ampleur et des répercussions des fraudes et des abus. Étant donné que le NAS constitue la voie d'accès à certains programmes fédéraux et provinciaux, les risques encourus par les contribuables en termes de versements excédentaires ou frauduleux sont considérables. Le vérificateur général a relevé dans son rapport plusieurs cas où des personnes ont obtenu des NAS après en avoir fait la demande et s'en sont servis pour produire de fausses demandes d'assurance-emploi; pour louer des véhicules à l'intention d'entreprises fantômes qui les envoyaient ensuite à l'étranger pour qu'ils soient vendus outre-mer, et pour demander et recevoir des remboursements illégitimes de TPS et d'impôt sur le revenu. Par conséquent, nous recommandons :

11. **Que DRHC instaure un plan démontrant qu'il est déterminé à ce que les cas de fraude et d'abus contre l'actuel système de NAS donnent lieu rapidement à des enquêtes menées avec efficacité. Ce plan devrait être présenté au Comité d'ici le 31 décembre 1999.**

---

10 Développement des ressources humaines Canada, Plan de travail 1998-1999 pour améliorer l'administration du NAS, pp. 4-5.

d'abus du NAS qui pourraient s'avérer coûteux pour les Canadiens en termes d'accès illégitime et inapproprié aux programmes fédéraux et provinciaux[8].

Les représentants de DRHC nous ont indiqué que le Ministère avait intensifié ses efforts pour expliquer l'écart au chapitre du nombre de décès enregistrés dans le RAS. Nous reconnaissons également que les provinces et territoires ont un rôle essentiel à jouer comme fournisseurs de statistiques démographiques pour le RAS. Par conséquent, nous recommandons :

6. **Que dans le but précis que le Registre d'assurance sociale soit exact et à jour, DRHC finisse de consulter d'ici le 31 décembre 1999, les gouvernements provinciaux et territoriaux au sujet de la divulgation contrôlée et prescrite des statistiques démographiques (naissances, décès et changements de nom) aux fins des échanges entre les gouvernements provinciaux et territoriaux et le gouvernement fédéral.**

7. **Que tous les échanges de statistiques démographiques effectués après les consultations soient approuvés par les commissaires à la protection de la vie privée des différentes instances compétentes, et que les résultats de ces consultations et de ces échanges figurent dans le rapport de rendement annuel de DRHC.**

Le processus entourant la preuve d'identité que doivent fournir les personnes qui demandent un NAS est une source de soucis supplémentaire relativement au nombre trop élevé de cartes en circulation et aux procédures de délivrance des nouvelles cartes. Aucune preuve d'identité n'était requise avant 1976, toutes les personnes désireuses d'avoir un NAS n'ayant qu'à remplir et à retourner un formulaire pour recevoir leur carte numérotée par la poste. C'est pour cette raison qu'en mars 1998, on dénombrait dans le RAS plus de 16 millions d'inscriptions qui n'étaient étayées d'aucun document d'identification[9].

Nous sommes d'accord avec le vérificateur général pour affirmer que les responsables du RAS devraient accorder plus d'attention aux actuelles procédures touchant la preuve d'identité. Comme le soulignait aussi le vérificateur dans son rapport, il est souvent difficile de vérifier l'information figurant dans les documents acceptés pour les demandes de NAS.

Nous prenons également en compte l'avis du commissaire à la protection de la vie privée du Canada selon lequel les procédures axées sur l'efficacité risquent d'avoir une incidence du côté de la protection des renseignements personnels. Un récent projet pilote mené par DRHC au Nouveau-Brunswick permet de vérifier en direct l'information fournie par les demandeurs de NAS au sujet de la naissance, du nom et des changements de nom (pour éviter la délivrance frauduleuse

---

8 Rapport du vérificateur général, chapitre 16, p. 16-13.

9 *Ibid.*, p. 16-15.

indiqué que les plaintes les plus fréquentes que son bureau recevait avaient trait à l'utilisation inappropriée du NAS dans le secteur privé. Les Canadiens en général et tout le secteur privé doivent comprendre leurs droits et responsabilités concernant le NAS. Par conséquent, nous recommandons :

5. **Qu'immédiatement après la promulgation de la loi sur le contrôle des cartes et des numéros d'assurance sociale, tous les ministères et organismes fédéraux compétents, de même que le commissaire à la protection de la vie privée du Canada orchestrent une campagne d'information publique au sujet des cartes d'assurance sociale au Canada. Cette campagne devrait :**

   - **Être destinée à la population, ainsi qu'aux entreprises, aux services et aux organismes oeuvrant dans le secteur privé;**
   - **Informer les citoyens quant aux utilisations légitimes de leur NAS, tant dans le secteur public que dans le secteur privé;**
   - **Informer les citoyens que la loi leur permet de refuser de divulguer leur numéro d'assurance sociale;**
   - **Informer les entreprises, les services et les organismes des contraintes imposées par la loi quant à l'utilisation qu'ils peuvent faire du numéro d'assurance sociale;**
   - **Joindre les Canadiens et Canadiennes par le truchement de différents moyens, notamment la presse écrite, la radio et la télévision.**

Les efforts visant à corriger les problèmes administratifs touchant le NAS doivent passer par le rétablissement de l'intégrité du Registre d'assurance sociale (RAS). Le RAS contient l'information fournie par toutes les personnes demandant un NAS : renseignements personnels de base comme les date et lieu de naissance et de décès et les noms du père et de la mère. Les Services nationaux, une direction générale de DRHC qui exerce ses activités à partir de Bathurst (Nouveau-Brunswick), administrent le RAS. Le vérificateur général a conclu que même si le registre est « généralement bien protégé et que sa sécurité matérielle est assurée », l'intégrité des données qu'on y trouve était menacée. Par exemple, on n'a consigné dans le RAS qu'un million de décès entre 1965 et 1990, alors que 4,4 millions de décès sont survenus au sein de la population canadienne. De plus, on a enregistré dans la base de données de 1998 du RAS 771 000 personnes de plus de 90 ans et 311 000 de plus de 100 ans, en comparaison de 127 000 et de 3 000, respectivement, dans le recensement de Statistique Canada. Toujours selon le RAS, dans le groupe d'âge des 20 ans et plus, la population totale est de 26 millions de personnes, plutôt que d'un peu plus de 22 millions, d'après les évaluations démographiques de Statistique Canada. Cela fait une différence énorme d'approximativement 4 millions de personnes. Étant donné que l'écart ne peut être expliqué, il existe un risque accru de fraude et

Statistique Canada à réaliser et à terminer d'ici le 31 décembre 1999 une étude sur les répercussions et l'ampleur de l'utilisation du NAS dans les secteurs public et privé. Les résultats de cette étude devraient être utilisés pour orchestrer une campagne d'information publique sur l'utilisation du NAS et sur les abus.

Le vérificateur général précise dans son rapport qu'un grand nombre de personnes sans statut juridique au Canada possédaient des NAS valables. Cette situation est imputable en partie à la délivrance de cartes de numéro d'assurance sociale temporaires (la série 900), à l'égard desquelles il n'y a pas de date d'expiration, ni sur les cartes elles-mêmes, ni dans le dossier pertinent du Registre d'assurance sociale. Ces cartes sont émises aux travailleurs saisonniers, aux étudiants étrangers et à des résidents non permanents comme les demandeurs du statut de réfugié. Elles sont également délivrées à des non-résidents canadiens qui effectuent des placements ou ont des activités bancaires au Canada, pour faciliter la production de leurs déclarations d'impôt. Comme le vérificateur le précise dans son rapport, plus de 680 000 cartes temporaires sont toujours actives après cinq ans, et le nombre de cartes de NAS temporaires attribuées représente plus du double du nombre de résidents non permanents recensés par Statistique Canada en 1997[7]. Manifestement, il faut s'attaquer immédiatement à ce problème, car la prolifération de ces cartes augmente les risques de fraude et d'abus. Nous ne souhaitons pas que les actuels détenteurs de cartes de numéro d'assurance sociale temporaires soient pénalisés, mais nous recommandons :

4. **Que DRHC veille à ce qu'on inscrive clairement une date d'expiration sur toutes les nouvelles cartes de numéro d'assurance sociale temporaires délivrées à compter du 1er janvier 2000. DRHC devrait également instaurer un mécanisme d'examen de toutes les cartes temporaires en circulation. Les détenteurs de ces cartes temporaires devraient pouvoir les conserver durant l'examen. Lorsque les groupes touchés auront été consultés, au plus tard le 31 décembre 1999, un rapport indiquant les résultats de cet examen, de même qu'un plan et un échéancier de remplacement des cartes temporaires en circulation devraient être présentés au Comité.**

Une conclusion générale ressort de nos audiences : la plupart des Canadiens et des Canadiennes ignorent les problèmes liés au NAS de même que l'ampleur et la possibilité des risques d'abus. Ils ne savent pas exactement à quel moment ils sont tenus de fournir leur numéro d'assurance sociale ni quand ils peuvent refuser de le divulguer sans encourir de conséquences. La même ignorance existe au sein des petits et grands services et entreprises du secteur privé. Le NAS constitue souvent pour eux un outil de tenue de livres pratique et économique, et leurs propriétaires et employés vont quelquefois demander leur NAS aux clients, voire exiger d'eux ce numéro, dans des situations tout à fait inappropriées. Certains iront même jusqu'à refuser un produit ou un service aux personnes qui refusent de divulguer leur numéro. Le commissaire à la protection de la vie privée du Canada nous a

---

7 Rapport du vérificateur général, chapitre 16, p. 16-17.

PARTIE 2 — GESTION ET CONTRÔLE DE L'ACTUEL SYSTÈME DU NAS

Les problèmes actuels touchant le numéro d'assurance sociale continuent de résider principalement dans l'imprécision de son objet. Conçu au départ comme un numéro de classement pour un nombre restreint de programmes gouvernementaux, la vocation du NAS n'était pas de devenir un système national d'identification personnelle des résidents du Canada ni d'être considéré comme tel. Or, c'est précisément ce qui s'est produit. Le Canada a maintenant un système de NAS qui s'apparente à un code national d'identification, sans être assorti du cadre de protection qui pourrait ou devrait l'entourer. Tous les experts de la protection des renseignements personnels nous ont affirmé que le Canada se trouve présentement dans la pire des situations, car il possède dans les faits un système national d'identification auquel aucun mécanisme de protection de la confidentialité n'a été greffé.

Il faudrait instaurer un mécanisme de contrôle officiel afin de régulariser l'utilisation du NAS. Légiférer peut donner des résultats, comme nous l'a démontré clairement le commissaire à l'information et à la protection de la vie privée de l'Ontario lorsqu'il a expliqué comment la *Loi de 1991 sur le contrôle des cartes Santé et des numéros de cartes Santé* avait réussi à prévenir les abus dans sa province. Cette loi a été mise en vigueur parallèlement à la délivrance des nouveaux numéros de cartes Santé en Ontario. En gros, la Loi dispose qu'on ne peut se servir de ces numéros qu'à certaines fins médicales prescrites. Toutes les utilisations autres que celles prévues dans la Loi constituent une infraction passible de sanctions sévères[6]. À ce sujet, nous recommandons :

2. **Qu'après avoir tenu les consultations appropriées, le gouvernement du Canada élabore une loi sur le contrôle des cartes et des numéros d'assurance sociale circonscrivant les utilisations légitimes de l'actuel NAS dans les secteurs public et privé et prescrivant des pénalités et des amendes en cas d'emploi inapproprié ou abusif du NAS. Un avant-projet de loi devrait être présenté au Comité au plus tard le 31 décembre 1999.**

Malgré les allégations concernant l'utilisation répondue et inappropriée du NAS dans le secteur privé, il n'y a pas d'étude qui confirme l'ampleur des abus, ni de fait des utilisations légitimes. Nous abondons dans le sens du commissaire à la protection de la vie privée de la Colombie-Britannique qui conclut qu'avant de concevoir des solutions qui pourront avoir du succès, il faut au préalable approfondir les questions de l'utilisation et de l'abus du NAS, en particulier dans le secteur privé. Par conséquent, nous recommandons :

3. **Que tous les ministères et organismes fédéraux compétents, ainsi que le commissaire à la protection de la vie privée du Canada travaillent avec**

---

6 Témoignages, réunion nº 47, 3 février 1999, p. 6.

Orientation de la réforme

Nos travaux nous ont amenés à conclure que les problèmes recensés par le vérificateur général relèvent de deux catégories distinctes qui doivent être traitées séparément par le gouvernement au moment de répondre au présent rapport et à d'autres rapports. La première concerne la « résolution » à court terme des lacunes du système actuel. Nous sommes convaincus que l'intervention à cet égard ne doit pas tarder. Par ailleurs, nous savons qu'une autre série de grands enjeux stratégiques doivent faire l'objet d'un examen. Ceux-ci ont trait à la question de savoir s'il y a lieu ou non de procéder à une refonte du système du NAS ou de le remplacer par un numéro d'identification commun. Si le débat à ce sujet doit s'amorcer maintenant, nous savons qu'une résolution exigera plus de temps et nécessitera une étude plus approfondie. Nous recommandons donc ce qui suit :

1. **En apportant des changements au système du numéro d'assurance sociale (NAS), le gouvernement du Canada doit intervenir simultanément à deux niveaux, c'est-à-dire qu'il doit :**

   A. **Prendre immédiatement des mesures pour mettre fin aux abus relevés dans la gestion et le contrôle de l'actuel système du NAS, comme l'y exhortent les recommandations de la partie 2 du présent rapport; et**

   B. **S'attaquer aux grands enjeux stratégiques à plus long terme touchant l'avenir du système du NAS, notamment aux problèmes de protection de la vie privée et de couplage de données.**

Nos collègues du Comité des comptes publics ont fait ressortir la nécessité de réagir rapidement à la première série d'enjeux et leurs recommandations font écho pour l'essentiel à ce que le rapport du vérificateur général considère comme des questions devant faire l'objet d'une attention immédiate et devant donner lieu à une recherche de solutions pratiques pour remédier aux problèmes du système actuel. Comme nous l'avons également indiqué, Développement des ressources humaines Canada, qui est le ministère responsable de la gestion et du contrôle du NAS, a élaboré un plan de travail général (voir l'annexe C) pour donner suite aux préoccupations du vérificateur général concernant le système actuel. Nos recommandations de la partie 2 visent à élargir et à étoffer ce travail.

En ce qui a trait au contexte stratégique général, nos audiences ont permis d'illustrer la portée et la complexité des enjeux en cause. La partie 3 de notre rapport met en lumière certaines de ces préoccupations. Plutôt que de formuler un grand nombre de recommandations définitives à cet égard, nous avons organisé notre rapport de façon à pouvoir mieux cerner le genre de questions qui, à notre avis, doivent être au cœur du débat parlementaire sur l'avenir du NAS au Canada.

- Examen de la procédure de demande;
- Examen de la gestion du Registre d'assurance sociale (RAS);
- Examen des méthodes d'enquête sur les cas de fraude et d'abus;
- Analyses approfondies de la base de données du NAS;
- Discussions avec des spécialistes de la protection des renseignements personnels et avec d'autres organismes intéressés au NAS;
- Entrevues avec des fonctionnaires de DRHC et d'autres ministères et agences fédéraux ayant des responsabilités en rapport avec le NAS de même qu'avec des organismes concernés à l'échelle provinciale.

L'étude du vérificateur général a fait ressortir un certain nombre de problèmes importants dans la façon dont le NAS est actuellement administré et contrôlé au Canada. En voici quelques-un :

- L'utilisation répandue du NAS dans les ministères et programmes fédéraux et provinciaux ainsi qu'à l'échelon municipal;
- La façon dont cette utilisation généralisée contribue aux possibilités de fraude et d'abus à l'égard des programmes gouvernementaux, avec les coûts financiers élevés que cela suppose pour les contribuables;
- La perception voulant que le NAS soit un code national d'identification plutôt qu'un simple numéro de dossier comme il était censé l'être à l'origine;
- L'utilisation répandue et abusive du NAS dans le secteur privé (à l'exception du Québec), qui accroît les possibilités de fraude, d'abus et d'atteinte à la vie privée;
- Les importants écarts relevés dans l'intégrité des données du Registre d'assurance sociale;
- L'insuffisance des efforts consacrés aux enquêtes relatives aux fraudes et aux abus mettant en cause le NAS;
- Les peines minimales imposées à l'égard de tels abus et fraudes;
- La prolifération de cartes d'assurance sociale temporaires sans date d'expiration;
- Les lacunes de la procédure de demande, notamment l'insuffisance des preuves d'identité exigées;
- La nécessité de réexaminer le cadre juridique et stratégique de gestion du NAS, notamment les questions relatives au couplage de données non autorisé et à la protection de la vie privée.

pour vérifier la solvabilité d'emprunteurs potentiels. Les provinces ont aussi commencé à utiliser le NAS aux fins de l'administration des prestations d'aide sociale. Les employeurs, petits et grands, s'en servent aussi dans leur système de suivi et de calcul des prestations des employés. Le secteur privé a commencé à tort à considérer le NAS comme une pièce d'identité. Ainsi, les propriétaires d'immeubles résidentiels obligent leurs locataires potentiels à le fournir sur leurs demandes de logement, les clubs vidéo s'en servent comme caution au moment de la location de films, les universités et les collèges l'exigent sur leurs formulaires de demande et les comptoirs de pizza s'en servent même comme numéro de client dans leur système de livraison. En plus de servir à des fins injustifiées, l'utilisation incontrôlée du NAS expose les Canadiens à de graves atteintes à leurs droits à la protection de leur vie privée pouvant prendre la forme d'un couplage de données effectué à leur insu et sans leur autorisation ou encore pouvant donner lieu à un vol d'identité.

Responsabilités fédérales à l'égard du NAS

Au sein du gouvernement fédéral, un certain nombre d'intervenants ont différents rôles et responsabilités à jouer en ce qui a trait au NAS. Comme nous l'avons indiqué, DRHC est l'« autorité responsable » du NAS. Il lui incombe à ce titre d'émettre les cartes, de faire enquête lorsque des abus sont soupçonnés et d'adapter la réglementation au besoin. DRHC gère aussi le Registre d'assurance sociale (RAS), dans lequel sont consignés les renseignements personnels fournis par les individus lorsqu'ils demandent une carte. Cette banque de données renferme tous les NAS actuellement en usage au Canada. La politique et les lignes directrices régissant la collecte et l'utilisation du NAS au sein des ministères et organismes fédéraux, notamment le couplage de données, relèvent de la compétence du Conseil du Trésor. Le ministère de la Justice soutient les autres ministères en leur donnant des conseils juridiques sur les questions relatives au NAS qui découlent de la *Loi sur la protection des renseignements personnels*, et il répond aussi aux demandes de renseignements générales que le public présente au sujet de l'utilisation du NAS par le secteur public et privé. Le commissaire à la protection de la vie privée assume les responsabilités de surveillance indépendante découlant de la *Loi sur la protection des renseignements personnels* et donne suite aux plaintes individuelles déposées au sujet de l'utilisation du NAS, lorsque celles-ci mettent en cause des atteintes à la vie privée. Étant un agent du Parlement, au même titre que le vérificateur général, le commissaire à la protection de la vie privée fait rapport directement au Parlement.

Rapport du vérificateur général : portée et conclusions

Le Bureau du vérificateur général a entrepris une vérification du système du NAS au Canada. La vérification visait d'abord à évaluer « la gestion et le contrôle du NAS pour déterminer s'ils sont efficients et efficaces et s'ils ont un fondement approprié dans la législation »[5]. Afin de satisfaire à cet objectif, les vérificateurs se sont attelés aux tâches suivantes :

- Examen du rôle et de l'utilisation du NAS dans la gestion des programmes sociaux et dans la perception des recettes;

---

5 Rapport du vérificateur général, chapitre 16, p. 16-10.

protection de la vie privée, de l'Advanced Card Technology Association of Canada, de l'Association des consommateurs du Canada, de l'Association des banquiers canadiens, d'Action réseau consommateur, de Revenu Canada, des Programmes de la sécurité du revenu (Développement des ressources humaines Canada). Nous avons reçu plusieurs mémoires, dont l'un d'Equifax, ainsi que des observations écrites de la part du commissaire à la protection de la vie privée de l'Ontario et du commissaire à la protection de la vie privée du Canada.

Au terme de nos travaux, nous avons de nouveau invité le ministère du Développement des ressources humaines pour qu'il reprenne avec nous le dialogue sur les observations recueillies et la façon de les mettre en pratique.

Au fur et à mesure de notre travail, notre inquiétude au sujet de la menace posée par l'actuel système du numéro d'assurance sociale pour la protection des renseignements personnels n'a cessé de croître. Nous avons aussi voulu examiner les répercussions des changements proposés à ce chapitre. Nous avons donc conclu en recueillant le témoignage de spécialistes de la protection qui nous ont donné des exemples pratiques de situations où la protection de la vie privée est actuellement compromise et nous ont indiqué celles auxquelles il était possible de remédier grâce à une réforme du système.

Plus ça change

Lorsque le système du NAS a d'abord été mis en œuvre en 1964, l'essentiel du débat a porté sur l'utilisation du numéro. Celui-ci allait-il simplement tenir lieu de numéro de dossier commun pour plusieurs programmes fédéraux de soutien du revenu/pensions ou s'il allait être un premier pas vers l'adoption d'un code universel d'identification pour les Canadiens? Le gouvernement au pouvoir à ce moment affirmait que le NAS n'a pas été conçu pour devenir un quelconque code d'identification universel. Il devait simplement demeurer un numéro de dossier pour consigner les cotisations et les prestations au titre des régimes de pensions du Canada/Québec, du Programme de la sécurité de la vieillesse et du Régime d'assurance-chômage.

Avec le temps, toutefois, l'utilisation du NAS s'est répandue tant à l'intérieur qu'à l'extérieur de l'appareil gouvernemental. D'abord, la *Loi de l'impôt sur le revenu* a autorisé l'utilisation du NAS comme numéro d'identification à des fins fiscales. Plus tard, la Loi a été modifiée pour obliger les particuliers à fournir leur NAS au moment d'acheter ou d'encaisser des obligations d'épargne du Canada. En conséquence, les institutions financières ont commencé à recueillir les numéros d'assurance sociale de leurs clients aux fins de la déclaration fiscale. Les Canadiens sont maintenant tenus d'avoir un NAS pour leurs enfants, s'ils veulent les inscrire au Régime enregistré d'épargne-études récemment mis en œuvre. De nos jours, au-delà d'une vingtaine de lois et règlements et sept programmes autorisent l'utilisation du NAS[4] (voir l'annexe B).

L'utilisation accrue du NAS au sein de l'appareil gouvernemental a bientôt eu pour effet d'en répandre l'utilisation dans le secteur privé. Bientôt, les bureaux de crédit ont commencé à l'utiliser

---

4 Rapport du vérificateur général, chapitre 16, p. 16-8.

Les membres du Comité reconnaissent aussi les mesures prises par Développement des ressources humaines Canada (DRHC) pour remédier à bon nombre des problèmes soulevés par le vérificateur général en ce qui concerne les numéros d'assurance sociale. Nous avons confiance dans la volonté du Ministère d'établir une stratégie pour remédier aux problèmes administratifs immédiats soulevés par le NAS. Toutefois, chaque fois que la situation le justifiait, nous avons demandé à DRHC d'adapter ses efforts pour tenir compte de nos préoccupations. Afin de l'obliger à rendre des comptes, nous lui avons fixé des échéanciers et imposé des exigences en matière de compte rendu. À notre avis, ces ajustements témoignent de la gravité des questions énoncées dans notre rapport et soulignent la portée de notre détermination à suivre l'évolution de ce dossier dans l'avenir immédiat.

Le présent rapport fait donc le lien entre le travail déjà accompli sur les mesures à prendre pour réformer le système du NAS au Canada dans l'immédiat, en plus de faire état de certaines des considérations essentielles de nature qui devrait éclairer le débat plus général portant sur les orientations futures.

Notre plan de travail

Nous avons établi notre plan d'étude de façon à pouvoir fonctionner efficacement sans faire double emploi avec le travail des autres ni le reproduire. Le Comité a ainsi tenu une série de séances d'information et de tables rondes auxquelles ont pris part les différents organismes gouvernementaux et non gouvernementaux concernés par l'administration actuelle et future des numéros d'assurance sociale. Ces discussions ont porté sur l'orientation stratégique générale.

Évidemment, le vérificateur général a été à l'origine de notre intérêt à l'égard de cette question et nous a donné un aperçu détaillé de son enquête et de ses conclusions. Nous avons ensuite réuni les différents organismes fédéraux concernés par l'administration du système du numéro d'assurance sociale et son fonctionnement général. Des hauts fonctionnaires du ministère du Développement des ressources humaines, qui est en quelque sorte le « port d'attache » du numéro d'assurance sociale, ont bien sûr été appelés à témoigner. Le Conseil du Trésor, qui est responsable des lignes directrices et des directives générales d'utilisation du numéro d'assurance sociale par les ministères et organismes fédéraux, ainsi que le ministère de la Justice, qui agit comme conseiller juridique auprès de tous les utilisateurs gouvernementaux fédéraux du numéro d'assurance sociale, ont eux aussi envoyé des représentants. Le commissaire à la vie privée du Canada, qui est un agent du Parlement au même titre que le vérificateur général, a assisté à cette séance pour nous faire part de ses idées sur l'utilisation du numéro d'assurance sociale et la nature des réformes qu'il serait souhaitable de mettre en œuvre.

Étant donné l'utilisation abondante du NAS par les différentes instances gouvernementales et par le secteur privé, nous avons ensuite tenu deux tables rondes avec le plus grand nombre d'intervenants qu'il nous a été possible de réunir. Nous avons ainsi entendu le témoignage des commissaires à la protection de la vie privée de l'Ontario et de la Colombie-Britannique, d'une administratrice municipale de la ville de Toronto responsable de l'accès à l'information et de la

attendre, leur rapport fait écho à bon nombre des recommandations du vérificateur général et fait allusion à certains des enjeux stratégiques généraux sur lesquels le Parlement et, en fait, les Canadiens, doivent se prononcer. Le Vingtième rapport du Comité des comptes publics stipule ce qui suit :

> Même si les vérificateurs [du Bureau du vérificateur général] y ont relevé [dans le programme du numéro d'assurance sociale (NAS)] quantité de lacunes, ces problèmes n'en sont pas moins subordonnés à la résolution de la question centrale touchant les objectifs du numéro d'assurance sociale. [. . .] La résolution du mandat du NAS est essentiellement une question politique qui devra faire l'objet d'une décision de la part du Parlement du Canada[3].

En plus de souscrire à cette conclusion, nous sommes assez d'accord avec les recommandations du Comité des comptes publics. Les nôtres y prennent d'ailleurs appui.

Mais puisque nous avons le mandat d'examiner les questions ayant trait au ministère du Développement des ressources humaines, qui est l'autorité responsable du NAS, et d'en faire rapport, nous avons aussi jugé bon d'aller au-delà des recommandations formulées par nos collègues. De plus, le Comité a tenu des audiences de plus vaste portée et entendu le témoignage d'un large éventail d'intervenants du gouvernement et de l'extérieur. Nous en avons profité pour procéder à une exploration préliminaire de certains des enjeux stratégiques généraux.

Malgré tout, à mesure que nos travaux progressaient, nous nous sommes rendus compte que nous manquions de temps pour effectuer l'étude approfondie des grandes questions stratégiques que sont la protection des renseignements personnels et le couplage de données — dont l'importance est cruciale pour l'avenir du NAS au Canada — qu'a menée l'ex-Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes. Ce comité a en effet consacré presque un an à la préparation de son rapport intitulé *La vie privée : Où se situe la frontière?* Déposé en avril 1997, ce rapport que l'on peut qualifier d'avant-gardiste, recense, explore et analyse un ensemble de questions complexes avec une créativité et une clarté remarquables. C'est avec une grande unanimité que le Comité a souscrit à un ensemble de recommandations étoffées et pris position en faveur de l'adoption d'une Charte canadienne des droits à la protection de la vie privée.

Hélas, la dissolution du Parlement en 1997 a soustrait le gouvernement à l'obligation de réagir globalement au rapport *La vie privée : Où se situe la frontière?*, comme le lui avait demandé le Comité des droits de la personne. Les questions et les recommandations qui y sont énoncées n'ont donc jamais fait l'objet d'une réponse officielle de la part du gouvernement. Notre Comité est d'avis que leur profondeur et leur portée touchent bon nombre des grands enjeux stratégiques examinés dans le cadre du débat sur l'avenir du NAS au Canada. Il ne faudrait pas que le gouvernement passe outre à un travail aussi ardu et important au moment de préparer sa réponse à nos travaux et à nos recommandations.

---

[3] Vingtième rapport du Comité permanent des comptes publics, *chapitre 16 du Rapport du vérificateur général du Canada de septembre 1998* (*La gestion du numéro d'assurance sociale*), 4 février 1999, p. 7.

Examen parlementaire

L'automne dernier, deux comités parlementaires se sont penchés sur différents aspects de l'administration et du cadre de fonctionnement du numéro d'assurance sociale. À la fin de novembre 1998, le Comité permanent du développement des ressources humaines et de la condition des personnes handicapées a entrepris une étude à ce sujet. Plus tard, le Comité permanent des comptes publics de la Chambre des communes a examiné le travail du vérificateur général, tenu des audiences sur la gestion du NAS au Canada et finalement déposé un rapport à la Chambre des communes le 4 février 1999. Nos travaux nous ont pour notre part amenés à réitérer la conclusion du vérificateur général, à savoir qu'une évaluation par le Parlement de l'actuel système du NAS au Canada s'impose et que les parlementaires ont un rôle crucial à jouer dans son orientation future.

Le rapport du Comité ne reprend pas les conclusions du vérificateur général. Nous reconnaissons le travail approfondi et détaillé accompli par son bureau, dont l'équipe de vérificateurs a fait ressortir un certain nombre de problèmes dans la façon dont le système du NAS est actuellement administré au Canada. Le rapport du vérificateur général renferme aussi une série de recommandations importantes pour remédier aux lacunes du système actuel. Le Comité est d'accord avec les conclusions du vérificateur général et appuie la teneur et l'esprit de ses recommandations.

Nous sommes toutefois conscients que le vérificateur général joue un rôle assez différent de celui des parlementaires et des comités parlementaires. Il lui incombe d'examiner le fonctionnement et l'efficacité des programmes gouvernementaux existants; il ne lui appartient pas de se prononcer sur les orientations stratégiques des programmes gouvernementaux, ni de formuler des recommandations sur la politique gouvernementale. Il ne participe pas non plus aux débats et aux décisions politiques; cette tâche nous incombe à nous, à titre de représentants élus. Le vérificateur général nous a d'ailleurs lui-même affirmé ce qui suit :

> Je pense que le moment est venu d'examiner les rôles, les objectifs et l'utilisation actuels du numéro d'assurance sociale.
>
> Le gouvernement devrait déterminer ce qu'il veut faire du numéro d'assurance sociale et, par la même occasion, étudier les autres options possibles. En outre, je crois qu'il est essentiel que le Parlement joue un rôle important dans la discussion de ces questions et dans la recherche d'une solution satisfaisante[2].

Au moment de rendre compte de nos délibérations, nous tenons également à souligner le travail accompli par nos collègues parlementaires du Comité des comptes publics. Comme on pouvait s'y

2 *Témoignages*, réunion nº 43, 4 novembre 1998, p. 2.

Rapport du vérificateur général du Canada — *La gestion du numéro d'assurance sociale*[1]. Étant donné la vaste portée de ses conclusions, le vérificateur général a jugé bon de demander au Parlement d'intervenir afin d'examiner l'administration et les enjeux stratégiques généraux associés à la carte et au numéro d'assurance sociale.

Outre les problèmes administratifs inhérents au système du NAS, les experts ont unanimement fait ressortir le danger posé par l'utilisation répandue du NAS dans le secteur privé et le fait que celle-ci dépasse maintenant sa fonction initiale de numéro de dossier aux fins des programmes gouvernementaux. Ajouter à la rapidité des progrès technologiques, cette situation a soulevé des inquiétudes quant à la possibilité d'un couplage de données non autorisé et inopportun d'un ministère fédéral à l'autre, au sein du secteur privé et peut-être même entre les secteurs public et privé. Bon nombre de ces couplages de données se font à l'insu des titulaires de cartes ou sans leur consentement éclairé. Ensemble, ces circonstances font ressortir l'importance de placer la vie privée et la protection des renseignements personnels au cœur de tous les débats sur le fonctionnement actuel du système du NAS et son avenir.

---

1 Ci-après désigné comme le Rapport du vérificateur général ou le chapitre 16.

INTRODUCTION

Au cours des dernières décennies, la vie quotidienne de l'ensemble des Canadiens s'est considérablement transformée. La rapidité sans précédent des changements technologiques a eu des conséquences inéluctables dans les domaines des communications, des affaires et du commerce, de l'éducation, des sciences, des voyages et du divertissement. L'adaptation à ces changements pose de grands défis aux Canadiens, à leurs représentants élus et à leurs gouvernements; nous devons repenser nos façons traditionnelles de « faire des affaires ». Parce que le commerce et la gestion des données, tant dans le secteur public que privé, relèvent maintenant plus du monde virtuel que du monde réel, les Canadiens doivent avoir l'assurance que les renseignements personnels à leur sujet sont en sécurité et que leur vie privée ne sera pas sacrifiée au profit de l'efficience. À bien des égards, le système de numéros d'assurance sociale est un exemple parfait de système gouvernemental devant satisfaire aux exigences du 21e siècle.

La plupart des résidents canadiens, dont un nombre croissant d'enfants, ont dans leur portefeuille une petite carte blanche sans photo où figure un numéro à neuf chiffres. Ce numéro, que l'on appelle le numéro d'assurance sociale (NAS), leur a été attribué au moment où ils ont commencé à travailler ou présenté une demande pour se prévaloir d'un programme gouvernemental.

Entre-temps, dans certains cas depuis plus d'une trentaine d'années, la plupart d'entre eux n'ont pas eu l'occasion de penser très souvent à leur numéro d'assurance sociale. Ils l'indiquent sur des demandes, l'inscrivent dans la case prévue à cette fin sur leur formulaire de déclaration d'impôt sur le revenu et le fournissent aux institutions financières au moment d'ouvrir un compte ou de demander un prêt ou une carte de crédit. Peut-être leur a-t-on demandé de l'indiquer et l'ont-ils utilisé comme numéro personnel d'identification au moment de payer par chèque, par exemple, chez leur épicier ou en guise de caution au moment de louer un film. La carte et le numéro d'assurance sociale n'ont apparemment aucune utilité pratique en soi; ils ne peuvent servir à acheter quoi que ce soit et ne garantissent pas non plus l'admission à un spectacle; ils ne peuvent être utilisés pour retirer de l'argent de la banque, ni servir à établir l'admissibilité de quelqu'un à un programme gouvernemental.

Il est récemment devenu évident que l'utilisation de la carte et du numéro d'assurance sociale, qui n'ont pas été modernisés depuis leur adoption en 1964, a des conséquences néfastes imprévues pour des milliers et peut-être même des millions de résidents canadiens. Ces derniers mois, plusieurs rapports ont fait état de graves problèmes et attiré l'attention sur l'évolution et l'utilisation du système des numéros et des cartes d'assurance sociale. L'ampleur et la nature de bon nombre de ces problèmes ont été rendues publiques avec la publication, en septembre 1998, du chapitre 16 du

TABLE DES MATIÈRES

LE COMITÉ PERMANENT DU DÉVELOPPEMENT DES RESSOURCES HUMAINES ET DE LA CONDITION DES PERSONNES HANDICAPÉES

a l'honneur de présenter son

QUATRIÈME RAPPORT

Conformément au paragraphe 108(2) du Règlement, le Comité permanent du développement des ressources humaines et de la condition des personnes handicapées s'est penché sur la gestion du numéro d'assurance sociale. À la suite des témoignages recueillis, le Comité a convenu de présenter le rapport suivant à la Chambre :

COMITÉ PERMANENT DU DÉVELOPPEMENT DES RESSOURCES HUMAINES ET DE LA CONDITION DES PERSONNES HANDICAPÉES

PRÉSIDENTE

Albina Guarnieri

VICE-PRÉSIDENTS

Dale Johnston

Bryon Wilfert

MEMBRES

Diane Ablonczy

Bernard Bigras

Bonnie Brown

Brenda Chamberlain

Hec Clouthier

Denis Coderre

Paul Crête

Libby Davies

Jean Dubé

Christiane Gagnon

John Godfrey

Larry McCormick

John O'Reilly

Hon. Andy Scott

Maurice Vellacott

GREFFIÈRE DU COMITÉ

Danielle Belisle

DIRECTION DE LA RECHERCHE PARLEMENTAIRE DE LA BIBLIOTHÈQUE DU PARLEMENT

Sandra Harder
William Young

Service des publications

AU-DELÀ DES CHIFFRES : L'AVENIR DU NUMÉRO D'ASSURANCE SOCIALE AU CANADA

Rapport du Comité permanent du développement des ressources humaines et de la condition des personnes handicapées

Albina Guarnieri, députée
présidente

mai 1999

Aussi disponible par Parliamentary Internet Parlementaire : http://www.parl.gc.ca

En vente: Travaux publics et Services gouvernementaux Canada — Édition, Ottawa, Canada K1A 0S9

CHAMBRE DES COMMUNES
CANADA

AU-DELÀ DES CHIFFRES : L'AVENIR DU NUMÉRO D'ASSURANCE SOCIALE AU CANADA

Rapport du Comité permanent du développement des ressources humaines et de la condition des personnes handicapées

Albina Guarnieri, députée
présidente

mai 1999